International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2017 IJSRCSEIT | Volume 2 | Issue 3 | ISSN : 2456-3307

Biometric System Introduction with its various Identification Techniques

Gaurav Patni*, Dr. Shilpa Sharma
School of Computer & Systems Sciences, Jaipur National University, Jaipur, Rajasthan, India

ABSTRACT

As per the traditional identification system for identifying any human being, there is easy way of marking the human using Biometric identification system. The paper presents the development of human identification system based on fingerprint identification. These ways of identifying any human will help us for securing his/her highly secure identification and personal verification. In order to tackle the increasing incidents of security breaches and frauds, every organization needs a full proof technology that can provide security and safety to individuals and the transactions that the individuals make. In a lot of articles, the researchers explores the need for biometrics in state and local governments, in the military, in commercial applications, Airports and Aircrafts to ensure the proper security system for identifying the human. Enterprise-wide network security infrastructures, government IDs, secure electronic banking, investing and other financial transactions, retail sales, law enforcement, and health and social services are already benefiting from Biometrics. Also here the various markets and the potential revenue are analyzed.

Keywords : Unique ID/IDs, biometric identification, biometric/biometric recognition, biometric registration/enrollment, verification procedure, template, transactions, fingerprint, law enforcement.

I. INTRODUCTION

The term Biometric means identifying the human on the basis of its Physiological and Behavioral traits. Biometric is the Unique identity of the person, using anyone of these, the identity can be verified very easily, if at the initial level the person is registered on the machine.

The authentication of the person is called identification process, by this the person/individual can be identified very easily in the group of people.

In the process of identification of any person we usually work with these –
Physiological Characteristics – It uses the shape or composition of the body include fingerprints, DNA, face, hand, retina, ear features and odour
Behavioral Characteristics – It uses the behavior of the person related to the pattern of the behavior of a person, such as typing rhythm, gait, gestures and voice.

Certain biometric identifiers, such as monitoring keystrokes or gait in real time can be used to provide continuous authentication instead of a single one-off authentication check.

As per the unique identity of each and every person, we can easily identify the person and manage the access control for them. With the biometric identification we can easily find and authenticate the individual on the basis of their physical or behavioral traits.

Biometric/Biometric Recognition
Automatically recognition of an individual based on their biological and/or behavioural characteristics.

Biometric Characteristics
On the basis of biological and behavioural characteristics of an individual, the biometric features can be extracted for the purpose of biometric recognition.

Biometric functionality
There are many different aspect of identifying/authenticate a person using biometric

concept, some of them are – human physiology, chemistry or behavior, etc.

For the uses of Biometric in any organization we have to see the particular software and hardware we are thinking about and additional to this the humanware (human) who is going to use it, these three must be balanced, if these are not balanced, then the technology we are using will not fulfill our organizational's requirements.

In my discussion with various organizations in Government - they were not ready to share data without permission from top authorities, in private – they want to keep their data safe and secure. Both were ready to discuss the problems verbally but not written.

I was able to locate seven such factors, that must be taken care for the properly assessing the suitability of any trait for use in biometric authentication –
Universality means every person who is using a system should possess the trait.
Uniqueness means the trait should be sufficiently different for individuals in the relevant population such that they can be distinguished from one another.
Permanence relates to the manner in which a trait varies over time.
Collectability related to the ease of acquisition or measurement of the trait.
Performance related to the accuracy, speed and robustness of the technology used.
Acceptability relates to how well individuals in the relevant population accept the technology such that they are willing to have their biometric trait captured and assessed.
Circumvention relates to the ease with which a trait might be imitated using an artifact or substitute.

There are two basic modes of a biometric system –
Authentication/Verification Mode –
The system performs a one-to-one comparison of a captured biometric with a specific template stored in a biometric database in order to verify the individual is the person they claim to be.
There are three step verification procedure –

- Reference Models for all the users are generated and stored in the model database
- Some samples are matched with reference models to generate the genuine and impostor scores and calculate the threshold.
- Testing step, in this process, we may use a smart card, username or ID Number (PIN) to indicate which template should be used for comparison.
    - Positive Recognition – It is a common use of the verification mode, where the aim is to prevent multiple people from using the same identity.
    - Negative Recognition – Where the system establishes whether the person is who he/she (implicitly or explicitly) denies to be.

Identification Mode -
In this mode, the system performs a one-to-many comparison against a biometric database in an attempt to establish the identity of an unknown individual.

The Identification mode can be used either for positive recognition or negative recognition.

The first time, when the individual uses a biometric system, it comes under enrollment phase, in the enrollment phase, biometric information from an individual is captured and stored in the system. In the further uses, biometric information is detected and compared with the information stored at the time of enrollment.

The first block (sensor) is the interface between the system and the real world, it has to acquire all the necessary data. It is an image acquisition system, but it can change according to the characteristics desired.

The second block performs all the necessary pre-processing : it has to remove artifacts from the sensor, to enhance the input.

The third block is necessary and important step as the correct features need to be extracted in the optimal way. In it a vector of numbers or an image with particular properties is used to create a template. A template is a synthesis of the relevant characteristics extracted from the source.

Working of template
During the enrollment phase, the template is simply stored somewhere (in card/database/both). During the matching phase, the obtained template is passed to a matcher that compares it with other existing templates,

estimating the distance between them using any algorithm. The matching program will analyze the template with the input. This will then be output for any specified use or purpose.

II. METHODS AND MATERIAL

Selection of biometric

The selection of biometrics in any practical application depending upon the characteristic measurements and user requirements. In selecting a particular biometric, factors to consider include, performance, social acceptability, ease of circumvention and/or spoofing, robustness, population coverage, size of equipment needed and identity theft deterrence.

Selection of a biometric is also based on user requirements considers sensor and device availability, computational time and reliability, cost, sensor size and power consumption.

Biometric verification becoming common

The Authentication by biometric verification is becoming increasingly common in the whole world now-a-days in almost all the place and in public security systems, consumer electronics, and point-of-sale applications. In addition to security, the driving force behind biometric verification has been convenience, as there are no passwords to remember or security tokens to carry. Measuring someone's gait doesn't even require a contact with the person.

Biometric devices, such as fingerprint readers, consist of:-

- A reader or scanning device.
- Software that converts the scanned information into digital form and compares match points.
- A database that stores the biometric data for comparison.

Accuracy of biometrics

The accuracy and cost of readers has until recently been a limiting factor in the adoption of biometric authentication solutions but the presence of high quality cameras, microphones, and fingerprint readers in many of today's mobile devices means biometrics is likely to become a considerably more common method of authenticating users, particularly as the new FIDO specification means that two-factor authentication using biometrics is finally becoming cost effective and in a position to be rolled out to the consumer market.

The quality of biometric readers is improving all the time, but they can still produce false negatives and false positives.

One problem with fingerprints is that people inadvertently leave their fingerprints on many surfaces they touch, and it's fairly easy to copy them and create a replica in silicone.

People also leave DNA everywhere they go and someone's voice is also easily captured. Dynamic biometrics like gestures and facial expressions can change, but they can be captured by HD cameras and copied. Also, whatever biometric is being measured, if the measurement data is exposed at any point during the authentication process, there is always the possibility it can be intercepted.

This is a big problem, as people can't change their physical attributes as they can a password.

While limitations in biometric authentication schemes are real, biometrics is a great improvement over passwords as a means of authenticating an individual.

Types of Biometrics

DNA Matching

Its a Chemical Biometric, in it the identification of an individual using the analysis of segments from DNA.

Ear

In Visual Biometric, the identification of an individual using the shape of the ear.

Eyes - Iris Recognition

In Visual Biometric, the use of the features found in the iris to identify an individual.

Eyes - Retina Recognition

In Visual Biometric, the use of patterns of veins in the back of the eye to accomplish recognition.

Face Recognition

In Visual Biometric, the analysis of facial features or patterns for the authentication or recognition of an

individuals identity. Most face recognition systems either use faces or local feature analysis.

Fingerprint Recognition

In Visual Biometric, the use of the ridges and valleys (minutiae) found on the surface tips of a human finger to identify an individual.

Finger Geometry Recognition

In Visual/Spatial Biometric, the use of 3D geometry of the finger to determine identity.

Gait

In Behavioural Biometric, the use of an individuals walking style or gait to determine identity.

Hand Geometry Recognition

In Visual/Spatial Biometric, the use of the geometric features of the hand such as the lengths of fingers and the width of the hand to identify an individual.

Odour

In Olfactory Biometric, the use of an individuals odour to determine identity.

Signature Recognition

In Visual/Behavioural Biometric, the authentication of an individual by the analysis of handwriting style, in particular the signature. There are two key types of digital handwritten signature authentication, Static and Dynamic. Static is most often a visual comparison between one scanned signature and another scanned signature, or a scanned signature against an ink signature. Technology is available to check two scanned signatures using advances algorithms. Dynamic is becoming more popular as ceremony data is captured along with the X,Y,T and P Coordinates of the signor from the signing device. This data can be utilised in a court of law using digital forensic examination tools, and to create a biometric template from which dynamic signatures can be authenticated either at time of signing or post signing, and as triggers in workflow processes.

Typing Recognition

In Behavioural Biometric, the use of the unique characteristics of a persons typing for establishing identity.

Vein Recognition

In Vein recognition, it is a type of biometrics that can be used to identify individuals based on the vein patterns in the human finger or palm.

Voice / Speaker Recognition

There are two major applications of speaker recognition:

Voice - Speaker Verification / Authentication

Auditory Biometric The use of the voice as a method of determining the identity of a speaker for access control.

If the speaker claims to be of a certain identity and the voice is used to verify this claim. Speaker verification is a 1:1 match where one speaker's voice is matched to one template (also called a "voice print" or "voice model"). Speaker verification is usually employed as a "gatekeeper" in order to provide access to a secure system (e.g.: telephone banking). These systems operate with the user's knowledge and typically require their cooperation.

For example, presenting a person’s passport at border control is a verification process - the agent compares the person’s face to the picture in the document.

Voice - Speaker Identification

Auditory Biometric Identification is the task of determining an unknown speaker's identity.

Speaker identification is a 1:N (many) match where the voice is compared against N templates. Speaker identification systems can also be implemented covertly without the user's knowledge to identify talkers in a discussion, alert automated systems of speaker changes, check if a user is already enrolled in a system, etc.

For example, a police officer compares a sketch of an assailant against a database of previously documented criminals to find the closest match(es).

In forensic applications, it is common to first perform a speaker identification process to create a list of "best matches" and then perform a series of verification processes to determine a conclusive match.

Note: There is a difference between speaker recognition (recognising who is speaking) and speech recognition (recognising what is being said). These two terms are frequently confused, as is voice recognition. Voice recognition is a synonym for speaker, and thus not speech, recognition. In addition, there is a difference between the act of authentication (commonly referred to as speaker verification or speaker authentication) and identification.

III. DISCUSSION

In the today's technology based society, slowly all our traditional individual authentication methods are gradually becoming obsolete. The Biometric authentication system is taking over traditional passwords or ID card based authentication due to numerous advantages.

Some important advantages of a biometric identification management system (which relies on "who you are") Vs traditional authentication methods (that rely on "what you have" or "what you know.") are as under -

Identification accuracy

The individual has unique physiological features that can't be easily swapped, shared, or stolen by any other person.

The biometric identification has the potential to accurately identify someone without a shadow of a doubt nearly 100% of the time.

The ability to accurately identify someone can be affected by environmental, age, or skin integrity issues, but with a multimodal biometric identification system we can eliminate those factors also. Multiple biometric attributes can identify someone with 100% certainty every time we scan them.

Biometrics reduces administrative costs

Biometric Hybrid Biometric Platform or Multi-Modal Biometrics System is used for the better identification of the human. Modern biometric identification management systems are comprised of hardware and software that are simple to install and easy to use. This reduces the need for intense training and ongoing management costs. Plus, biometric identification management helps save other costs such as the issuance of new ID cards, and replacing lost or damaged ID cards. Biometric identification also generates cost savings for IT by eliminating the time consuming and resource draining need to reset passwords. If you use single sign on solutions to log in to your network, think about the IT time and cost of password resets every time an employee forgets their password. In addition, if that password gets stolen, it can lead to a security breach.

Establishes accountability

Each and every action or transaction will be recorded and clearly documented by the individual associated with it which reduces the possibility of system misuse and fraud.

Adds convenience

Due to the fact that passwords can be forgotten or easily guessed and the fact that ID cards can be damaged, swapped, or shared, biometrics are more convenient because individual physiological attributes are always with you.

Difficult to forge

Biometric attributes are almost impossible to forge or duplicate. Even if you manage to forge a biometric attribute such as a fingerprint, modern biometric devices with liveness detection have the capability to identify a fake from the original.

Improved Return on Investment (ROI)

Compared to traditional identification systems that may rely on passwords, ID cards, or personal identification numbers (PINs), the ROI is much higher with biometric identification systems.

Seamless Integration

Biometric identification systems can be seamlessly integrated with workforce management time and attendance systems, access control, surveillance, and visitor management solutions – all managed through a single window on a computer. Biometrics provides centralized control for security administrators.

IV. CONCLUSION

As we discussed above the Biometric identification management systems offer higher security, convenience, accountability, and accurate audit trails. If these agenda items are top of mind for the success of your business.

, now is the time to learn more about the advantages of implementing biometric identification management.

V. REFERENCES

[1]. Shelly Batra, Sandeep Ahuja, Abhishek Sinha, and Nicholas Gordon, 2012 in Proceedings of M4D 2012 28-29 February 2012 New Delhi, India, "eCompliance : Enhancing Tuberculosis Treatment with Biometric and Mobile Technology", pp 35-40, 2012

[2]. Michael Paik, Navkar Samdaria, Aakar Gupta, Julie Weber, Nupur Bhatnagar, Shelly Batra, Manish Bharadwaj, and William Thies, 2010 , in Proceeding NSDR'10 Proceedings of the 4th ACM Workshop on Networked Systems for Developing Regions, Article No. 4, "A Biometric Attendance Terminal and its Application to Health Programs in India", pp 1-6, 2010

[3]. Nupur Bhatnagar, Abhishek Sinha, Navkar Samdaria, Aakar Gupta, Shelly Batra, Manish Bhardwaj, and William Thies, 2012 in Springer, "Biometric Monitoring as a Persuasive Technology : Ensuring Patients Visit Health Centers in India's Slums", pp. 169-180, 2012

[4]. Seema Rao, and Prof. K.J.Satoa, 2013, in International Journal of Advanced Research in Computer Science and Software Engineering, Vol 3, Issue 4, "An Attendance Monitoring System Using Biometrics Authentication", pp. 379 – 383, April 2013

[5]. O. Shoewu, and O.A.Idowu, 2012, in The Pacific Journal of Science and Technology, Vol 13, No. 1, "Development of Attendance Management System using Biometrics", pp. 300-307, May 2012 (Spring)

[6]. Tiwalade O. Majekodunmi, and Francis E. Idachaba, 2011, in Proceedings of the World Congress of Engineering WCE – 2011, July 6-8, 2011, London, U.K., Vol II, "A Review of the Fingerprint, Speaker Recognition, Face Recognition and Iris Recognition Based Biometric Identification Technologies", 2011

[7]. Michael H. Indico, Luisa M. Lanciso, and Ana L. Vargas, 2014 , in International Journal of Scientific and Research Publications, Vol 4, Issue 1, "Mobile Monitoring and Inquiry System Using Fingerprint Biometrics and SMS Technology", pp. 1-6, January 2014

[8]. Pallavi Verma, and Namit Gupta, 2013, in International Journal of Science and Research (IJSR), Vol 2, Issue 10, "Fingerprint Based Student Attendance System Using GSM", pp. 128 – 131, October 2013

[9]. Hemangi Kulkarni, Aniket Yadav, Darpan Shah, Pratik Bhandari, and Saumya Mahapatra, 2012, in Int. J. Computer Technology & Applications, Vol 3 (2), "Unique ID Management", pp. 520-524, 2012

[10]. K. Jaikumar, M. Santhosh Kumar, S. Rajkumar, and A. Sakthivel, 2015 , in International Journal of Research in Engineering and Technology, Vol 4, Issue 2, "Fingerprint Based Student Attendance System with SMS Alert to Parents", pp. 293-297, Feb 2015

[11]. Smita S. Mudholkar, Pradnya M. Shende, Milind V. Sarode, "Biometrics Authentication Technique for Intrusion Detection Systems Using fingerprint Recognition", in International Journal of Computer Science, Engineering and Information Technology (IJCSEIT), Vol 2, No. 1, pp. 57-65, February 2012

[12]. Gowthami P, and Dr. P. Sathishkumar, 2016 , in International Journal of Innovative Research in Advanced Engineering (IJIRAE), Vol 3, Issue 4, "An Andriod Based Patient Monitoring System", pp. 54-57, April 2016

[13]. Mohd Idzwan, Mohd Salleh, Mohamad Rahimi, Mohamad Rosman, Raja Abdullah, and Raja Yaacob, 2011, in International Conference on Computer Applications and Industrial Electronics (ICCAIE 2011) - IEEE, "Biometric Authentication for Securing Life Cycle Management of Electronic Patient Records", pp. 602-606, 2011

[14]. Abhishek Sinha, Shashank Batra, Dr. Shelly Batra, and Sandeep Ahuja, 2014, in Indian Journal of Medical Informatics – official Organ of Indian Association for Medical Informatics (IAMI), "Using Biometrics to Turn the Tap Off of Multi Drug Resistant TB (MDR TB)", pp.38-41, 2014

[15]. Adebayo Omotosho, Omotanwa Adegbola, Barakat Adelakin, Adeyemi Adelakun, and Justice Emuoyibofarhe, 2014 , in Journal of Biology, Agriculture and Healthcare, Vol 4, No. 18, "Exploiting Multimodal Biometrics in E-Privacy Scheme for Electronic Health Records", pp. 22-33, 2014

[16]. Shirish Joshi, 2016, in International Journal for Scientific Research & Development (IJSRD), Vol 3, Issue 11, "BIOMETRICS : Selecting the Best Solution", pp. 206-208, 2016

[17]. Jayant V. Kulkarni, Bhushan D. Patil, and Raghunath S. Holambe, 2006 , in Pattern Recognition Society : Published by Elsevier Ltd., "Orientation feature for fingerprint matching", pp. 1551-1554, 2006

[18]. Mangesh Raut, Sheetal Kokate, Sandeep Shinde, Sushant Karpe, and Mr. Sachin Barahate, 2015 , in International Journal for Scientific Research & Development (IJSRD), Vol 3, Issue 1, "Virtual Biometric Fingerprint Attendance System", pp. 511-513, 2015

[19]. Nitin Sambharwal, and Dr. Chander Kant, 2015, in International Journal for Scientific Research & Development (IJSRD), Vol 3, Issue 2, "Biometrics Fingerprint Sensors : An Introduction", pp. 1019-1025, 2015

[20]. Divya K V, Akansha Pandey, Manoj Sharma, Meghashrita Kashyap, and Divya Kumari, 2016, in International Journal for Scientific Research & Development (IJSRD), Vol 3, Issue 12, "A Survey on Biometric Authentication for Accident Victims During Emergencies" pp. 992-994, 2016

[21]. Chirag Singh Sisodia, Aparajiit Shrivastava, 2015, in International Journal for Scientific Research & Development (IJSRD), Vol 3, Issue 9, "A Survey on Network and Security Authentication using Biometrics", pp. 236-241, 2015

[22]. Keerti Arse, 2014, in International Journal for Scientific Research & Development (IJSRD), Vol 2, Issue 9, "A Survey of Automated Biometric Authentication Techniques", pp. 906-908, 2014

[23]. Anjana P, Betty P, 2015, in International Journal for Scientific Research & Development (IJSRD), Vol 2, Issue 12, "An Elaborated View on Biometric Template Protection", pp. 490-495, 2015

[24]. Koichi Ito, Ayumi Morita, Takafumi Aoki, Tatsuo Higuchi, Hiroshi Nakajima, and Koji Kobayashi, 2005, in ICIP – IEEE International Conference, "A Fingerprint Recognition Algorithm Using Phase-Based Image Matching for Low-Quality Fingerprints", pp. II-33 – II-36, 2005

[25]. Rubal Jain, Dr. Chander Kant, 2015, in International Journal for Scientific Research & Development (IJSRD), Vol 3, Issue 2, "Attacks on Biometric Systems : An Overview", pp. 1090-1094, 2015

[26]. Eshraf El-Sisi, 2011, in The International Arab Journal of Information Technology, Vol 8, No. 4, "Design and Implementation Biometric Access Control System Using Fingerprint for Restricted Area Based on Gabor Filter", pp. 355-363, October 2011

[27]. Adewole K.S., Abdulsalam S.O., Babatund e R.S., Shittu T.M., and Oloyede M.O., 2014, in Computer Engineering and Intelligent Systems, Vol 5, No. 2, "Development of Fingerprint Biometric Attendance System for Non-Academic Staff in a Tertiary Institution", pp. 62-70, 2014

[28]. Norshidah Katiran, Helmy Abdul Wahab, Jamal Rasyid, and Abdul Rahman, 2010 , " in Proceedings of EnCon2010 3rd Engineering Conference on Advancement in Mechanical and Manufacturin g for Sustainable Environment April 14-16, 2010, Kuching, Sarawak, Malaysia, "Development of Attendance System using Biometric Fingerprint Identification pp. 1-4, 2010

[29]. Hemlata Patel, and Pallavi Asrodia, 2012, in International Journla of Electrical, Electronics and Computer Engineering, vol1, No. 1, "Employee Attendance Management System Using Fingerprint Recognition", pp. 37-40, 2012

[30]. Oloyede Muhtahir O., Adedoyin Adeyinka O., and Adewole Kayode S., 2013, in International Journal of Applied Information Systems (IJAIS), Vol 5, No. 3, "Fingerprint Biometric Authentication for Enhancing Staff Attendance System", pp. 19-24, February 2013

[31]. Devendra Kumar Yadav, Sumit Singh, Prof. Shashank Pujari, and Pragyan Mishra, 2015, in International Journal of Advanced Research in Electrical , Electronics and Instrumentation Engineering, Vol 4, Issue 6, "Fingerprint Based Attendance System Using Microcontroller and LabView", pp. 5111-5121, June 2015

[32]. Ravi Subban, and Dattatreya P. Mankame, 2013, in Lecture Notes on Software Engineering, Vol 1, No. 2, "A Study of Biometric Approach Using Fingerprint Recognition", pp. 209-213, May 2013