ISSN 2349-6193
Impact Factor: 3.866

IJESMR

International Journal OF Engineering Sciences &Management Research

A BRIEF REVIEW OF DIFFERENT BIOMETRIC AUTHENTICATION SYSTEM BASED ON ITS BENEFITS, DRAWBACKS AND EASE OF COMFORT IN USE

Shital Baghel*[1] & Thaneshwar Kumar Sahu[2]

[*1&2]Assistant Professor, Department of Biomedical Engineering and Bioinformatics, Chhattisgarh Swami Vivekanand Technical University, Bhilai

Keywords: *Biometric, Unimodal biometric system, Multimodal biometric system, Face recognition, Authentication.*

ABSTRACT

Security is the most important thing which every living organism wants. We as a human being are much worried about our personal belongings and for that we are using models which are based on passwords and PINs. But these are easily hacked by impostors hence a fraud happens but the biometric authentication system has overcome all these drawbacks and this paper aims to give a brief review about this physiological biometric authentication techniques, along with its benefits, drawbacks, how can it be used easily and its future scope.

INTRODUCTION

The word biometrics comes from the ancient Greek words: bios life and metros measure. Humans use inputs such as voice, face, gait to recognize each other is well-known. In many emerging technologies, Recognition of people based on their characteristics is important. Now a days in a wide variety of applications biometrics is used to confirm the identity of an individual that require the identification or verification schemes. Automatic identification/verification of an individuals' identity based on the analysis of his/her biological (biometric) traits is broadly known as biometrics technology [1].Hence an automatic personal recognition system based on behavioral or physiological characteristics is defined as biometrics. Biometrics use biological properties of a human like hand geometry, voice, face, iris, and fingerprints to identify individuals. In our everyday lives Automatic and accurate identity validation is becoming increasingly critical in areas like traveling, healthcare, financial transactions, access control, and many others. Traditionally items such as passwords, PIN numbers, ID cards and tokens were used for automatic Identity recognition. Despite the wide deployment of such tactics, the means for authentication is either entity-based or knowledge-based which raises serious concerns with regard to the risk of identity theft. Biometric modalities are difficult to steal or counterfeit when compared to PIN numbers or passwords. In addition, the convenience of not having to carry a piece of ID or remember a password makes biometric systems more accessible and easy to use.

This is the age of universal electronic connectivity i.e., the electronic world with its applications like e-banking, e-commerce, e-government, virtual shops, e-mail, etc. There are obstacles and some problems related to it like unauthorized access, hackers, viruses, computer theft, etc, which affect the productivity and prosperity of individual or group. Thus, security became necessary as well as important. The solution for this problem is Authentication meaning the verification of the message and of the user. Therefore in complex society, necessity of personal identification in the e-world is increasing, and the authentication of the user is a challenge that must stop the fraud in advanced technologies. Techniques related to biometrics authentication is divided in to two categories broadly as Physiological Biometric and Behavioral Biometric which is further classified in to Passive and Invasive as shown in Fig1. Algorithms are used in Physiological biometrics methods to define identity in terms of data gathered from direct measurement of the human body like palm prints, finger scan, Finger print, hand geometry, retina scanning, Iris and facial geometry. In Behavioral biometrics a specific action of a person is used for analysis such as signature dynamics, motion recognition, voice Identification, and keystroke dynamics. In an Invasive Biometric the subject has to participate actively in enrolling into the system as well as during subsequent identification. The willing participation of the subject in the controlled environment of these systems is intrinsic to the success of the identification. Hand geometry technologies, Retina scanning technologies, Signature recognition technologies, Fingerprint technologies are its examples.

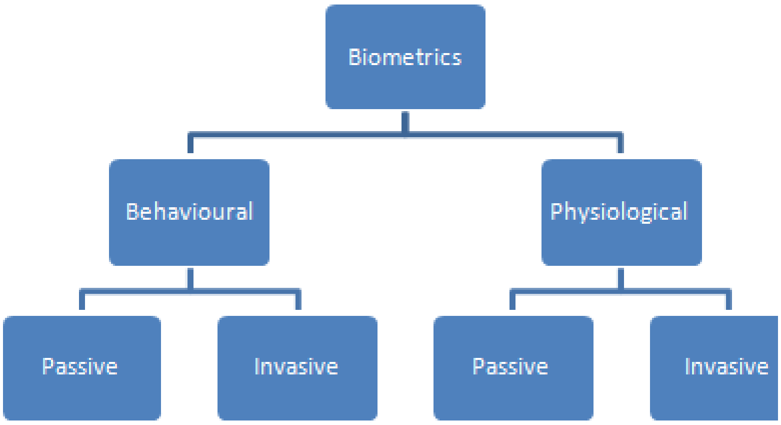

Fig1: Biometrics Method

A user's active participation is not required in Passive biometrics and can be successful without a person even knowing that they have been analyzed. Examples include, Iris recognition technologies (limited), Facial recognition (truly passive), and Voice recognition technologies (limited).

HOW BIOMETRIC SYSTEM WORKS

In a, biometric systems a set of specific vectors are compared with a set of models from a database. It is a recognition systems which captures biometric features from a person based on a model and extracts vectors.

There are four important elements in a common biometric system as shown in Fig.2.

- First one is Sensor module which captures the biometric data of an individual. An example is a camera that captures face of a user.
- Second is Feature extraction module in which feature values are extracted from the acquired data. The position and orientation of minutiae points in a face image would be extracted in the feature extraction module of a image processing system.
- Third one is the Matching module in which comparison is done between the feature values with those in the template by generating a matching score. For example, in this module, the number of matching minutiae points between the query and the template will be computed and treated as a matching score.
- Last one is the Decision module in which the user's identity is established or a claimed identity is either accepted or rejected based on the matching score generated in the matching module[2]

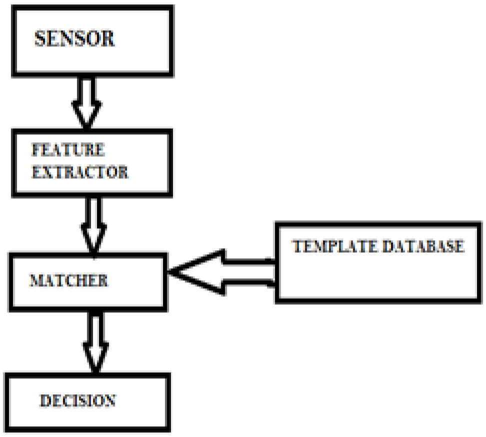

Fig2: Biometrics Authentication System

BIOMETRIC AS PHYSIOLOGICAL AUTHENTICATION SYSTEM

Here we will discuss different physiological biometric authentication ,given below are such authentication systems:

1. Face Recognition

For long time facial features like nose ,chin,eyes ,lips of human have played a significant role in the recognition of individuals. Face Recognition System (FRS) are very popular now a days because of unique shaping of each person’s face and is a popular method in biometric recognition area as shown in Fig3. Different software’s are used to do the real identification of human facial features. There are two ways for the facial authentication, in the first one a photo camera is used for collecting a set of images via which we do static recognition of persons facial features and in the second one we use video camera for real time identification of persons. Then template are created for each sample from the captured image and matching process is taken for the recognition process[3].

There is a lot of scope in future development of face recognition system, we can improve it using 3D camera for data collection, more accurate sensors to capture image can be used. Visual spots, lines and other unique patterns can be seen using these methods.

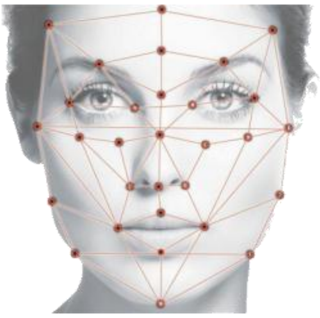

Fig3: Scanned Face recognition sample

Benefits: It is easy to use and its system implementation cost is low.

Drawbacks: There are number of factors which affect the overall performance face recognition system. For examples, light conditions quality or resolution of collected photos for each individual, angles of face rotation, etc. Also, different facial expressions such as sad expression, happy, angry and others impose some challenges on the automatic recognition of people identities [3,4,5].

2. Palm Recognition

For the identification/verification of their legitimate users many security systems and applications depend on the recognition of hand geometry. In various security sectors it has gained a wide popularity. Since the late of 60s it is used as biometric method [6,7]. By scanning the hand area using a specific scanner measurements of the hand-geometry is obtained in order to composite an accurate sample three-dimensional scanning is done in different angles for better feature extraction as shown in Fig.4 [3]. In order to reduce the overall cost of features extraction work on simplifying the sensor device is going on is the current improvement.

Fig4: Palm recognition sample

Benefits: It is more friendly authentication system and it has wide acceptance by participants than other biometric systems.

Drawbacks: For storing the scanned information of palm geometry large space is required [8]. Wearing some jewelries may impact the extraction of palm information, a special hardware device for scanning the hand geometry, a three-dimensional scanner is needed to acquire full information of the palm[5].

3. Fingerprint Recognition

Each person has a different print on each finger. Even identical twins have different prints on each ones finger. Among other biometrics security methods for both of identification and verification processes fingerprint based biometric authentication systems became one of the most conducted, popular and successful authentication techniques of one's' identity. Biologically, the pattern of a fingerprint surface is basically classified into three main patterns are loop, arch and whorl [8]. The two main fingerprint characteristics are the valleys and ridges on the finger surface which are used to distinguish between two individuals because they have specific followings in their direction and locations on the fingerprint. By using a scanner fingerprint formation is collected. Fig.5 shows a sample of fingerprint.

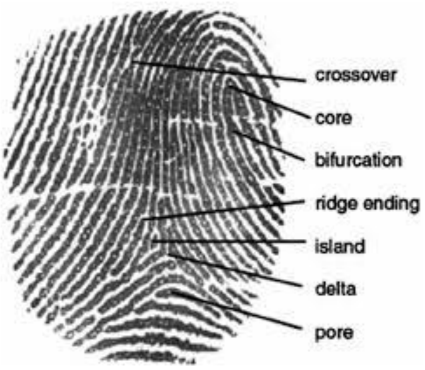

Fig5: Scanned Fingerprint sample

Benefits: In thousands of institutions for the security purposes deploying fingerprint recognition has been increasing because of the ease of use of this method by the users , the low cost of implementation since the optical sensor is a cheap device [8,9], and does not require so much power [10].

Drawbacks: To obtain high quality image of finger patterns a complex biometric system is required. Cuts,tear and wear, issues of dirt effect the ridges and minutiae of fingertip[5,10].

4. Ear Recognition

Ear features extraction and also matching processes is done in ear recognition. Specific measurements of outlook of the ear is used for actual recognition in which unique template is created by using a mathematical model. Fig 6 shows different features in a ear.

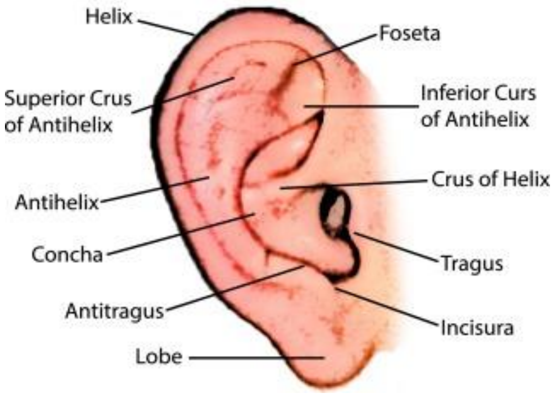

Fig6: Ear features sample

Benefits: It is more comfortable and friendly.

Drawbacks: This method has not achieved a remarkable level of security yet. One of the disadvantages of ear recognition is the simple distinguished features of the ear that cannot provide a strong establishment of an individual's identity [4].

5. Iris Recognition

Iris is located centrally in eye and is colored circular part of eye as shown in Fig6. Every individual has different iris pattern. First of all iris image is being captured via a special camera then the general process of identifying and verifying a person is done and then iris image is passed to the data analysis for extraction of features for each sample and is prepared for authentication process.

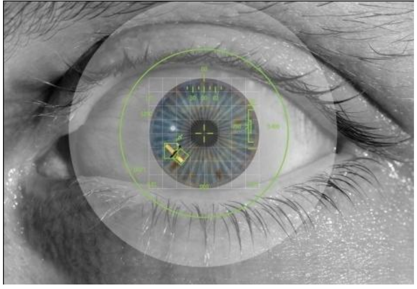

Fig7:Iris sample

Benefits: Due to the widespread of iris scanners in different security sectors it is an optimal method for the automatic authentication of individuals. A proper level of reliability is achieved in iris recognition. Use of flexible operating scanners makes this device in more demand[11].

Drawbacks: Some of these factors are wearing glasses, eye lenses and etc. are number of factors which creates different issues in iris recognition and this method is very expensive.

CONCLUSION AND FUTURE WORK

Various authentication systems is an essential requirement now a days, this paper overviewed different types of authentication systems and also summarized its benefits and drawbacks. A lot of future developments can be done in order to increase accuracy and reliability of these authentication system, such as combining palm and iris recognition or combining finger print and face recognition etc.

REFERENCES

1. *Yanushkevich, S.N., "Synthetic Biometrics: A Survey," in Neural Networks, 2006. IJCNN '06. International Joint Conference on, vol., no., pp.676-683, 0-0 0*
2. *A. Zahid., (2012), "Basic Structure of A Biometric System",Security Of Multimodal Biometric Systems Against Spoof Attacks, University Of Cagliari, Cagliari, Pp 12-13.*
3. *Eng, A.; Wahsheh, L.A., "Look into My Eyes: A Survey of Biometric Security," in Information Technology: New Generations (ITNG), 2013 Tenth International Conference on, vol., no., pp.422-427, 15-17 April 2013.*
4. *Kataria, A.N.; Adhyaru, D.M.; Sharma, A.K.; Zaveri, T.H., "A survey of automated biometric authentication techniques," in Engineering (NUiCONE), 2013 Nirma University International Conference on, vol., no., pp.1-6, 28-30 Nov. 2013.*
5. *Dharavath, K.; Talukdar, F.A.; Laskar, R.H., "Study on biometric authentication systems, challenges and future trends: A review," in Computational Intelligence and Computing Research (ICCIC), 2013 IEEE International Conference on, vol., no., pp.1-7, 26-28 Dec. 2013.*
6. *Liu, Simon; Silverman, M., "A practical guide to biometric security technology," in IT Professional, vol.3, no.1, pp.27-32, Jan/Feb 2001.*
7. *Delac, K.; Grgic, M., "A survey of biometric recognition methods," in Electronics in Marine, 2004. Proceedings Elmar 2004. 46th International Symposium, vol., no., pp.184-193, 18-18 June 2004.*
8. *Zaeri, N. (2011). Minutiae-based fingerprint extraction and recognition. INTECH Open Access Publisher.*
9. *Faundez-Zanuy, M., "Biometric security technology," in Aerospace and Electronic Systems Magazine, IEEE, vol.21, no.6, pp.15-26, June 2006.*

10. *Weizhi Meng; Wong, D.S.; Furnell, S.; Jianying Zhou, "Surveying the Development of Biometric User Authentication on Mobile Phones," in Communications Surveys & Tutorials, IEEE, vol.17, no.3, pp.1268-1293, thirdquarter 2015.*
11. *Liu, Simon; Silverman, M., "A practical guide to biometric security technology," in IT Professional, vol.3, no.1, pp.27-32, Jan/Feb 2001*