International Journal of Advanced Research in

Computer Networking,Wireless and Mobile Communications

Volume: 2 Issue: 1 05-May-2015,ISSN_NO: 2320-7248

Biometric Recognition Techniques

Anjana Doshi[1], Manisha Nirgude[2]

ME Student, Computer Science and Engineering, Walchand Institute of Technology Solapur, India[1]

Asst. Professor, Information Technology, Walchand Institute of Technology Solapur, India[2]

ABSTRACT- *Information Security has also made by advances in the field of Information Technology. Verification plays an important role in the process of Information security. The password method is the cheapest and simplest technology, because it only requires simple software resources. In the case of traditional password based verification systems if a password is discovered by an unauthorized user it can be easily hacked. Hence biometric recognition system is used. Various researchers have proposed a number of biometric techniques for personal verification. Biometric techniques include such type of software which one does not need to remember or carry a token. For recognition purpose Biometric based personal authentication systems use physiological or behavioural factors of a person. This paper is review on the biometric authentication techniques and some future possibilities in this field.*

Keywords: Biometrics, Biometric Technology, System Performance, Classification

1. INTRODUCTION

For recognizing the human characters, Biometrics is a science and technique is physiological as well as behavioural. In these systems physiological traits include iris recognition, fingerprint, face recognition, retina scan, palm print, hand geometry, DNA, voice etc and on the other hand behavioural traits includes typing rhythm, key stroke, pattern, handwriting etc [1] [2]. Due to the increasing requirement of highly reliable personal identification and authentication in a number of government and commercial applications, there has been remarkable growth in biometric recognition technology few past years. In various applications like in ATM's for more secure transaction, airports for security purposes, driving licenses and many other personal certificates authentication of person is becoming increasing popular which is based upon biometric verification. A block diagram of biometric Recognition System is shown below in fig 1 [3]. There are two main parts of biometric recognition system. First one is enrolment in which is first template gets stored in database and in the second process of the individual's data is compared with the acquired templates.

The block diagram illustrates the two basic modes of a biometric system [4] [5]. First, in 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. Second step is identification mode in that system performs a one-to-many comparison against a biometric database in attempt to establish the identity of an unknown individual.

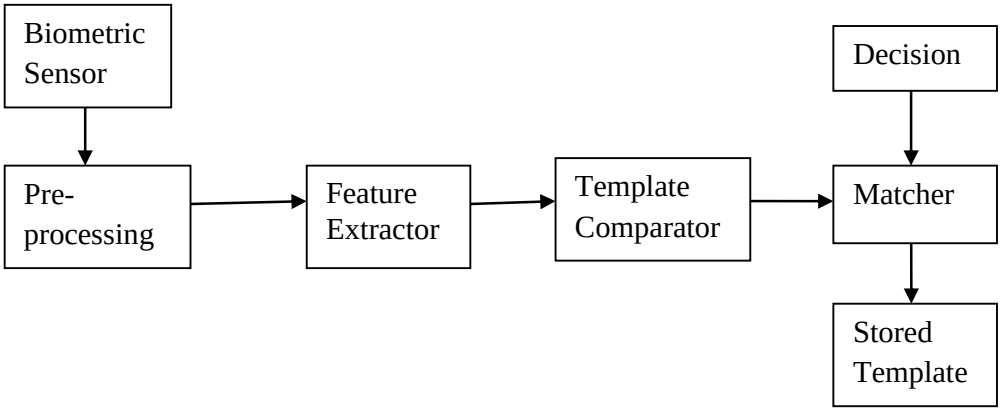

Fig1 Block diagram of general Biometric Detection System

2. BIOMETRIC TECHNOLOGY

In Biometrics-based authentication have many usability advantages over traditional systems such as passwords. Specifically, users can never lose their biometrics, and the biometric signal is difficult to steal or forget. Biometric technologies are defined as, "automated methods of verifying or recognizing the identity of a living person based on physiological or behavioural characteristic". The term automated methods refers to three basic methods in concern with biometric devices:

1. A mechanism to scan and capture a digital or analogy image of a living personal characteristic;
2. Compression, processing and comparison of the image to a database of stored images; and
3. Interface with applications systems.

2.1 Advantages of Biometrics:

1. Biometric traits cannot be lost or forgotten while traditional password can lost or forgotten.
2. Biometric traits are difficult to copy, share and distribute while traditional password can be easy to copy.
3. They require the person being authenticated to be present at the time and point of authentication.

2.2 Biometric Features [3]

1. Uniqueness: Uniqueness means it has an identical trait and which won't appear in two people.
2. Universality: Universality means it occur in as many people as possible.
3. Performance: Performance means it don't change over time that is it remains same for life time.
4. Measurability: Measurability means it is measurable with simple technical instruments.
5. User friendliness: are easy and comfortable to measure.

3. BIOMETRIC SYSTEM PERFORMANCE:

There are two types of errors which evaluates the performance of biometric system. First one is matching errors and second is acquisition errors. These are explaining as follows [4].
The matching errors consist of the following:

3.1 False Acceptance Rate (FAR):

In FAR number of false acceptance is divided by the total number of identification attempts. If there is mistaking of biometric measurements from two different people to be from same people is known as FAR.

3.2 False Rejection Rate (FRR):

It is the percentage of times the system produces a false reject. If there is mistaking of biometric measurements from same people to be from two different people is known as FRR.

The acquisition errors consist of the following:

3.3 Failure to Capture Rate (FTC):

It is proportion of attempts for which a biometric system is unable to capture a sample of sufficient quality.

3.4 Failure to Enroll Rate (FTE):

It is proportion of the user population for which the biometric system is unable to generate reference templates of sufficient quality. This includes those who, for physical or behavioural reasons, are unable to present the required biometric feature.

3.5 Receiver operating characteristic or relative operating characteristic (ROC):

The ROC plot is a visual characterization of the trade off between the FAR and the FRR. In general, the matching algorithm performs a decision based on a threshold which determines how close to a template the input needs to be for it to be considered a match. If the threshold is reduced, there will be fewer false non-matches but more false accepts.

Conversely, a higher threshold will reduce the FAR but increase the FRR. A common variation is the Detection error trade off (DET), which is obtained using normal deviation scales on both axes. This more linear graph illuminates the differences for higher performances.

3.6 Equal error rate or crossover error rate (EER or CER):

The rate at which both acceptance and rejection errors are equal. The value of the EER can be easily obtained from the ROC curve. The EER is a quick way to compare the accuracy of devices with different ROC curves. In general, the device with the lowest EER is the most accurate.

3.7 Template capacity:

It is the maximum number of sets of data which can be stored in the system.
All of the above are used to calculate the accuracy and performance of a biometric system.

4. CLASSIFICATION OF BIOMETRICS:

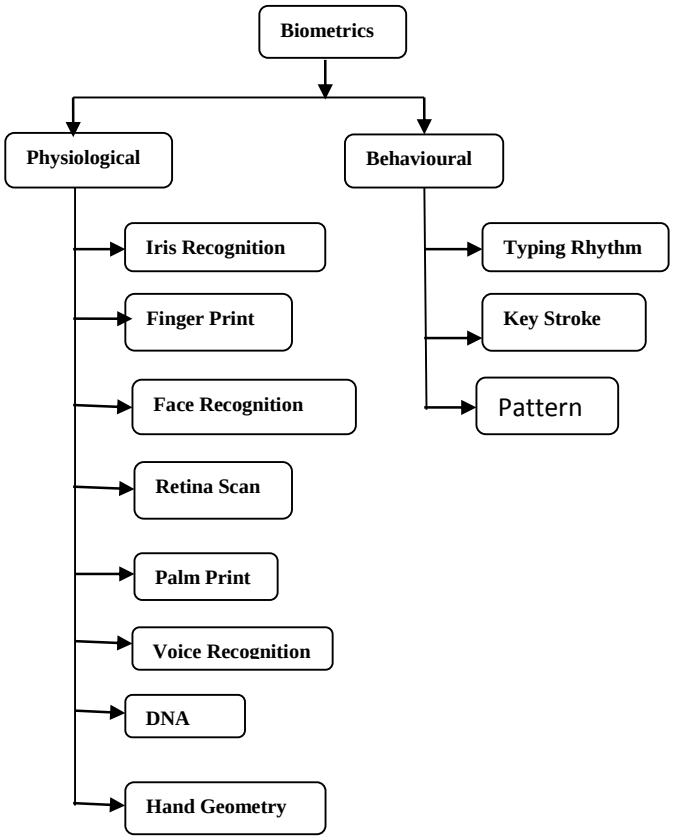

Fig 2 Classification of Physiological and Behavioural characteristics of Biometrics

Fig 2 shows the classification in Biometric. Biometrics encompasses both physiological and behavioural characteristics [5]. A physiological Characteristic is a relatively stable physical feature such as iris pattern, finger print, and retina pattern , iris recognition , palm print, hand geometry, DNA, or a Facial feature and on the other hand behavioural traits in identification is a person's signature, keyboard typing pattern or a speech pattern, handwriting etc. The degree of interpersonal variation is smaller in a physical characteristic than in a behavioural one.

A number of biometric characteristics exist and are in use in various applications. There are some strengths and weaknesses of each biometric, and the choice depends on the application. No single biometric is expected to effectively meet the requirements of all the applications. Some of them are explained below.

4.1 TYPES OF BIOMETRICS

4.1.1 Iris Recognition*:*

Many authors analysed Iris Recognition System. Conclusions of some of them are as follows [10] [11]. This recognition method uses the iris of the eye which is the colour area that surrounds the pupil. Iris patterns are thought unique. The iris patterns are obtained through a video-based image acquisition system. Iris scanning devices have been used in personal authentication applications for several years. Systems based on iris recognition have substantially decreased in price and this trend is expected to continue. The technology works well in both verification and identification modes. Current systems can be used even in the presence of eyeglasses and contact lenses. The technology is not intrusive. It does not require physical contact with a scanner. Iris recognition has been demonstrated to work with individuals from different ethnic groups and nationalities. Fig 3 shows the parts of eye image.

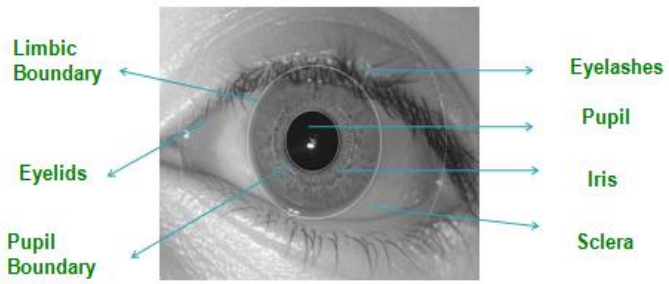

Fig3 Eye Image

Advantages of iris recognition:

1) Protected internal organ hence less prone to injury
2) Highly stable over lifetime

Disadvantages of iris recognition:

1) Difficult to capture for some individuals

2) Problems occurs due to eyelashes, lens and reflections from the cornea

4.1.2 Fingerprints:

Many authors analysed Fingerprints Recognition System. Conclusions of some of them are as follows [12] [13]. Fingerprints are unique for each finger of a person including identical twins and the patterns of any one individual remain unchanged throughout life. Fingerprint recognition device is most commercially available for biometric technologies which s is used for desktop and laptop access and it is widely available from many different vendors at a low cost. With these devices, users no longer need to type passwords instead; only a touch provides instant access. Fingerprint systems can also be used in identification mode [6]. Fig 4 shows features of fingerprint.

Fig 4Fingerprint

Advantages of finger print recognition:

1) Easy to use
2) Systems require less space

4.1.3 Face Recognition*:*

Many authors studied Face Recognition System and they conclude something based on it as follows [14]. Face recognition technologies analyse the unique shape, pattern and positioning of facial features. The face is natural biometric because it is a key component in the way we humans remember and recognize each other. The identification of a person by their facial image can be done in a number of different ways such as by capturing an image of the face in the visible spectrum using an inexpensive camera or by using the infrared patterns of facial heat emission. The most popular approaches to face recognition are based on either (i)the location or shape of facial attributes, such as the eyes, eyebrows, nose, lips, and chin and their spatial relationships, or (ii)the overall analysis of the face image that represents a face as a weighted combination of a number of canonical faces [7].Facial recognition in visible light typically model key features from the central portion of a facial image. Using a wide assortment of cameras, the visible light systems extract features from the captured image that do not change over time while avoiding superficial features such as facial expressions or hair. Fig 5 shows the face image.

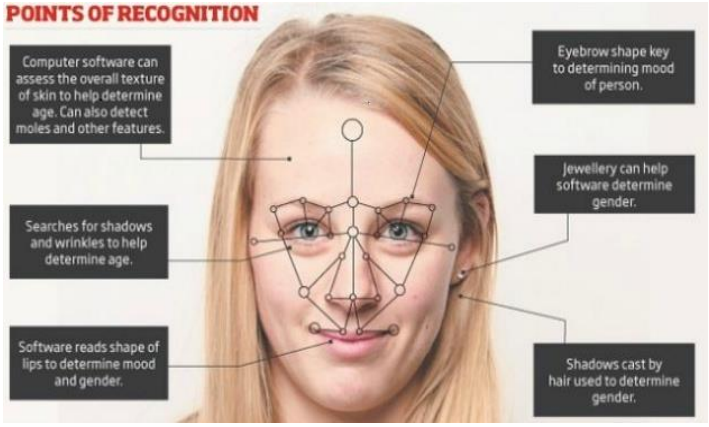

Fig-5 Face

Advantages of face recognition:

1) No contact required for recognition
2) Commonly available cameras used

Disadvantages of face recognition:

1) Sensitive to changes in lighting, expression
2) Faces change with time

4.1.4 Voice Recognition:

Many authors studied Voice Recognition System and they conclude something based on it as follows [15]. Voice recognition is a technology through which sounds, phrases and words voiced by human beings are transformed into electrical signals, and then these signals are converted into code design [9]. Here we emphasize on the human voice because we generally and most often use voices to communicate our thoughts, our ideas with others in surrounding environment [8].

Advantages of Voice recognition:

1) Public acceptance
2) No highly unique

Disadvantages of Voice recognition:

1) Difficult to control sensor and channel variances that significantly impact capabilities
2) Not sufficient for identification over large databases

4.1.5 Signature Verification:

Many authors studied Signature Verification and they conclude something based on it as follows [16]. Signature verification is based on pattern. This technology uses the dynamic

analysis of a signature to authenticate a person. The technology is based on measuring speed, pressure and angle used by the person when a signature is produced. One focus for this technology has been e-business applications and other applications where signature is an accepted method of personal authentication. Fig 6 shows signature.

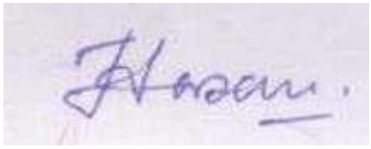

Fig 6 Signature

Advantages of Signature Verification:

1) Fast and simple training
2) Cheap hardware
3) Little storage requirement

Disadvantages of Signature verification:

1) Signature Verification is designed to verify subjects based on the traits unique signature. As a result, individuals who do not sign their names in a consistent manner may have difficulty enrolling and verifying in signature verification

Comparing with other biometric recognition, Iris recognition most suitable technique [6] [7] [8] [9]. The iris has unique features and is complex enough to be used as a biometric signature. It means that the probability of finding two people with identical iris patters is almost zero. According to Flom and Sapir the probability of existence of two similar irises on distinct persons is 1 in 10^{72}.

It has following exclusive characteristics [10].

1] Uniqueness of the Iris: No two irises are same. The iris is unique because of the chaotic morphogenesis of the organ. Even the two twins can be distinguished easily.

2] Stability over time: Iris is one of the most carefully protected organs in one's body. The features of the iris remain stable and fixed from about one year of age until death.

3] Discriminating the imposter: Changing the size of the pupil can distinguish the iris between live and dead.

CONCLUSION

Comparing with other biometric recognition, Iris recognition most suitable technique. Iris has unique property. Hence we will use Iris Recognition System in our project.

REFERENCES

[1] C.B. Tatepamulwar, V.P. Pawar, H.S. Fadewarr, "**Biometric Recognition**", NCI2TM: 2014

[2] Shweta Gaur, V.A. Shah, Manish Thakker, "**BiometricRecognition Techniques**", International Journal ofAdvancedin Electrical, Electronics and Instrumentation Engineering,Vol. 1, issue 4, October 2012.

[3] K P Tripathi, "**A comparative Study of Biometric Technologies with Reference to Human Interface**",International Journal of Computer Applications, Volume 14- No.5, January 2011.

[4] Anil K. Jain, Arun Ross and SalilPrabhakar," **An Introduction to Biometric Recognition**" Appeared inIEEE Transactions on Circuits and Systems for Video Technology,Special Issue on Image- and Video-BaseBiometrics, Vol. 14,No. 1, January 2004.

[5]Anil K. Jain, Arun Ross and SalilPrabhakar (2004), "AnIntroduction to Biometric Recognition."

[6]Comparisons of Various Biometric Technologies, www.biometricvision.com

[7]AlinaKlokova, "Comparison of Various BiometricMethods".

[8] RabiaJarfi and Hamid R. Arabina, "A Survey of FaceRecognition Techniques", Journal of Information ProcessingSystems, Vol.5, No.2, June 2009.

[9]Jain, A.K.; Ross, A.; Pankanti, S, "Biometrics: a tool forinformation security" Information Forensics and Security,IEEE Transactions on Volume: 1, Issue: 2 Digital ObjectIdentifier: 10.1109/ TIFS.2006.873653 Publication Year:2006, Page(s): 125 –143

[10]Y. Zhu, T. Tan and Yusag, "Biometric PersonalIdentification based on Iris Patterns, pattern Recognition",15th Internal Configuration, vol. 2, pp 801-804, 2004.

[11]John Daugman, "**How Iris Recognition Works**," IEEE Conference on ICIP, 2002, pp. I–33– I–36

[12]PrateekVermaetl,"**Feature Extraction Algorithm ofFingerprint Recognition**", International Journal ofAdvanced Research in computer science and software Engineering,Volume-2, Issue 10 October 2012.

[13] L. Hong and A. K. Jain, "Integrating faces and fingerprintsfor personal identification", IEEE Trans. PatternAnal.Mach. Intell., Volume 20, No. 12, Dec. 1998, pp.

[14] A. S. Tolba, A.H. El-Baz, and A.A. El-Harby, "**FaceRecognition**", World Academy of

Science, Engineering andTechnology, Vol: 2 2008-07-21

[15] Bhupinder Singh, RupinderKaur, NidhiDevgun, RamandeepKaur," **The process of Feature Extraction inAutomaticVoice Recognition System for Computer Machine Interaction with Humans**", InternationalJournal of Advanced Research in Computer Science and Software Engineering, Volume 2, Issue 2, February 2012

[16] SamitBiswas, Tai-hoon Kim, Debnath Bhattacharyya, "**Features Extraction and Verification of SignatureImageusing Clustering Technique**", International Journal of Smart Home, **Vol**-4 No.3, July 2010.