ISSN 2278 - 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering
Vol. 1, Issue 4, October 2012

Biometric Recognition Techniques: A Review

Shweta Gaur[1], V.A.Shah[2], Manish Thakker[3]

M.Tech. Scholar, Department of Instrumentation and Control Engineering, Dharmsinh Desai University, Nadiad, Gujarat, India[1].

Professor and Head, Department of Instrumentation and Control Engineering, Dharmsinh Desai University, Nadiad, Gujarat, India[2].

Assistant professor, Department of Instrumentation and Control Engineering Dharmsinh Desai University, Nadiad, Gujarat, India[3].

Abstract: In today's world automation is encompassing virtually every walk of life and human control functions are delegated to technical equipment. No doubt this results in emerging requirement of highly reliable personal identification system for authenticated access of resources and to reject imposters. Traditional password based verification systems can be easily hacked when a password is divulged to an unauthorized user. A number of biometric techniques have been proposed for personal identification by various researchers. Biometric includes something which one does not need to remember or carry a token. Biometric based personal authentication systems use physiological or behavioral traits of a person for recognition purpose. Physiological traits include fingerprint, face, hand geometry etc. and behavioral traits are speech, handwriting, key strokes etc. During past few years, there has been remarkable growth in biometric recognition technology due to the increasing requirement of highly reliable personal identification and authentication in a number of government and commercial applications. In this paper we present a comparative study of various biometric recognition techniques suggested for authentication purpose and to reject imposters.

Keywords: Authentication, Biometric, Feature extraction, Template Matching.

I. INTRODUCTION

Biometrics is a science and technique for recognizing the human characters, both physiological and behavioural. Authentication of person based upon biometric verification is becoming increasingly popular in various applications like banking, aviation, financial transactions etc. A block diagram of biometric Recognition System is shown in Fig-1. The main functioning of such system involves two parts; enrolment and test. During the enrolment process, template gets stored in database. And during test process, the individuals data is compared with the acquired templates. Matching program evaluates template with input, estimating distance between these two using suitable algorithm. This is considered as the output for specified purpose.

First block, known as sensor acts as an interface between system and real world and acquires necessary data. Vision based picture acquisition system are convenient choice for it, but can be changed as per application. Second block performs preprocessing, i.e. removes artefacts from sensor and enhances input picture. In the next block, essential characteristics are extracted. This is a critical stage the right features are required to be extracted in optimal way. Image features or vector of the numbers with specific properties is used for formation of template. Template is combinational set of related features extracted from source. Elements of biometric measurements those are not required for comparison algorithms are banished in templates for reducing size of file and for protecting identity of claimer.

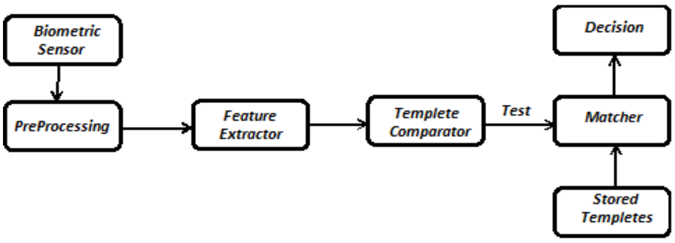

Fig.1. Block diagram of general Biometric Detection System

II. PHYSIOLOGICAL TRAITS

Physiological traits are related to the physical structure of a person. Variety of physical properties related to human body are utilized for authentication purpose, like fingerprints, facial and hand geometry, iris, retina, vascular patterns etc. Most of these detections are vision based.

1. Finger Prints

Finger print detection involve either detection of minutiae i.e. ridge ending, bifurcation, dot or an island (as can be seen in Fig-2), or vision based pattern matching for recognition.

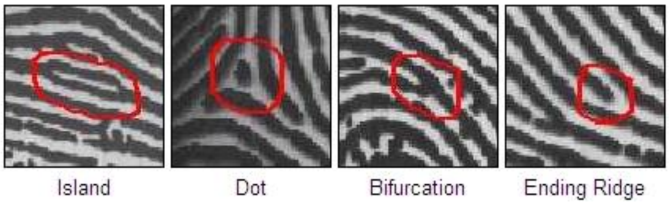

Fig.2. Minutiae patterns of finger print

Minutiae based techniques depends upon the detection of minutiae location and direction for detection whereas pattern matching compares two images to judge the similarities.

1.1 Techniques used for reading finger print are based upon optical, capacitance, thermal or ultrasonic principles [1].

1.1.1 Optical techniques rely on capturing the digital image formed by the reflection of light from the points where ridges touches the sensor's touch surface. Optical fingerprint readers comprise of a light source, light sensor, touch surface where inger is placed and a capture device which can be a CCD (Charge Coupled Device), a CMOS camera or may be a simple webcam.

1.1.2 Capacitive type finger print sensors consist of an array of capacitive plates on a silicon chip. One plate of capacitor is formed by the finger, other plate contains a tiny area of metallization on the chip. When finger is placed against the surface of chip, the ridges of finger are close to the nearby pixels and so have high capacitance. The valleys are atcomparatively distant from the pixels and so have lower capacitance.

1.1.3 Ultrasonic method uses high frequency sound waves to monitor the finger surfaces, the user places the finger on a piece of glass and the ultrasonic sensor moves and reads whole finger print. The finger-tip is applied to a window of ultrasonic head. The head contains one, two or a ring shaped matrix of electro-acoustic transducers. Ultrasonic method of acquiring fingerprint is based on sending ultra sonic signals towards the finger and detecting the echo.

1.1.4 Thermal technique is mainly useful for the detection of latent finger prints. Research showed that eccrine rich and sebaceous rich latent print impression on paper may be made visible by application of heat between 220°C to 300°C. When this heated substrate of paper is observed under illumination in 505nm range of light the latent prints can be made visible.

1.2 Fingerprint detection technique offers following benefits-

1.2.1 It provides high distinctiveness. All human beings have distinct fingerprints. Identical twins, who have same DNA patterns, have different finger prints. Therefore fingerprints are a strong authentication mechanism.

1.2.2 The fingerprint patterns i.e. ridges are formed in the womb and remain invariant through lifetime except in case of deep injury.

1.2.3 Except for an amputee humans has legible fingerprints so can be easily authenticated without the need of carrying a token.

1.2.4 It's a widely accepted technique.

1.3 The limitation includes false reproduction of fingerprints, subjected to noise and distortion because of dirt and twists. Also some people do not find it appropriate to place their fingers on the same place which is been touched by so many other peoples.

2. Facial recognition

Facial recognition can be regarded as a computer application for authenticating a person from a digital image or from a video capture. This technology relies on mapping of the specific facial features like the distance between eyes, nose width, length of jaw line etc. These are referred as nodal points and are measured by creating numerical code which is a face print for any individual. This face print represents a face in the database. Both 2D and 3D techniques are used for automated facial recognition systems.

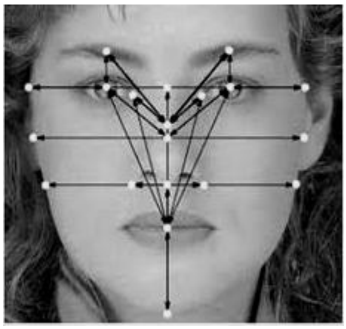

Fig.3. Nodal points of Face

2.1 2D Facial Recognition

In this a 2D image of face is compared with one of that stored in the data base. The image is captured with a camera and is represented as a vector of intensities. This vector is then approximated as a sum of basis vectors (eigen faces) computed by principal component analysis from a database of face images. These principal components represent the typical variations seen between faces and provide a concise encapsulation of the appearance of a sample face image, and a basis for its comparison with other face images[2]. From this processed image, features are extracted. This extracted feature is referred as facial code or face template. Template is then compared with database and similarities are determined. For accuracy the image should be captured with face looking directly to the camera. Problems can be there with little variance of light or facial expression from the images in the data base. As compared to 3D facial recognition technique it needs lesser storage space for identification templates, so is a faster process. 2D images contain limited information, and are sensitive to orientation, expressions, illumination and facial make over.

2.2 3D Facial Recognition

3D image recognition uses a real time capture of facial image and uses the features of face like curves of eye socket, nose and chin where rigid tissue and bone is most apparent. As this technique uses the depth and an axis of measurement that is not affected by lighting, it can be utilized to recognize a subject at different view angles (Fig-4).

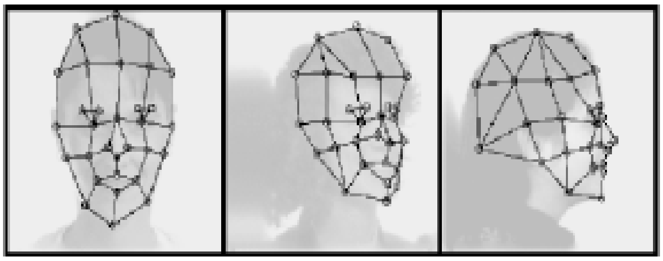

Fig.4. Features for 3D recognition

Accuracy of facial representation is high with the ability to capture and store more information. Use of 3D data provides much better handling of illumination and orientation related variations.

The computational cost is high as large amount of data is to be processed.

3. Iris Recognition

The iris of the eye is the coloured annular area that surrounds the pupil (Fig-5). Iris patterns are unique. No two irises are same, even right and left eye of same person.

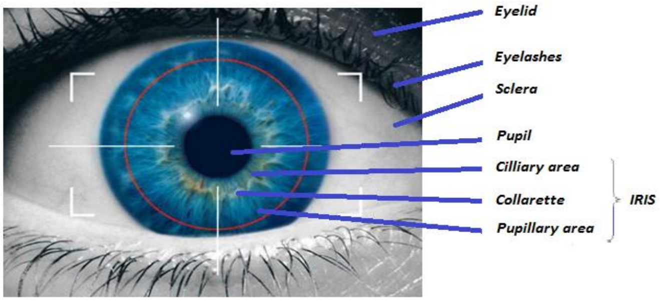

Fig.5. Iris

Iris detection method may involve image acquisition, localization, segmentation and matching. High resolution iris image is required for authentication purpose, so a camera with such capabilities and high frame transfer rate or video capturing device can be used. After acquiring iris image, localization step is performed. By this the iris portion of image is detected. This can be approximated by two circles, one is the iris/sclera (outer) boundary, and another interior to the first is the iris/pupil (inner) boundary [3]. Iris Localization is followed by segmentation which can be defined as the process of separating the input iris image in to several components. After iris localization and segmentation the final step is pattern matching of the iris image with the stored templates from the database.

This technique of person authentication is highly accurate and iris patterns do not change over time. Acquisition of iris image makes this method difficult for implantation with ease as it requires proper alignment and positioning. Also the change in pupil size with change in light conditions may affect the results.

4. Hand Geometry and Palm print

4.1 Hand geometry based identification systems utilize the geometric features of the hand like length and width of the fingers, diameter of the palm and the perimeter. Vision based techniques are utilized for authentication purpose. It includes image acquisition, feature extraction, template matching, as in the case of any other biometric technique. Image acquisition for hand biometrics may contact type and guided one, which require a flat platform to place the hand and pegs to guide the placement of the user’s hand, or platform-free, non-contact techniques. Constrained and contact based. Systems requiring a flat platform and pegs or pins to restrict hand degree of freedom Unconstrained and contact based. Peg-free scenarios, although still requiring a platform to place the hand. Unconstrained and contact-free. Platform-free and contact-less scenarios where neither pegs nor platform are required for hand image acquisition[4].

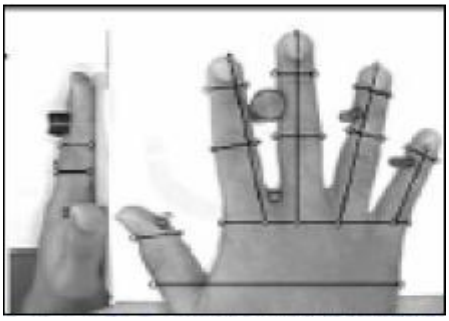

Fig.6. Hand Geometry

4.2 Palm prints are series of dark lines representing peaking portions of the friction ridged skin. Either minutiae based techniques which depends upon the location, direction, and orientation of minutiae points or ridge based matching which utilizes ridge patterns features such as sweat pores, spatial attributes and geometrical characters can be used. Like in the case of fingerprint technique capacitive, optical or ultrasonic sensors can be used.

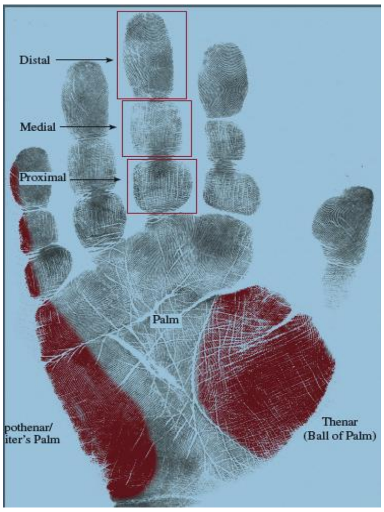

Fig.7. Palm Print for biometric detection

5. Retina Recognition

Retina to the eye is like film is to the camera. It has millions of photoreceptors which transforms light rays into electrical impulses.

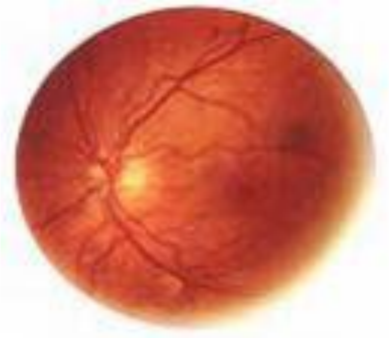

Fig.8. Human Retina

Retina based recognition technique uses blood vessel pattern in the retina which is unique for an eye. As retina is on the back side of eye, so it is not directly visible and that's why stable over the lifetime of a person. Further because of this reason an infrared light source is necessary to illuminate the retina. Advantage of infrared light is that the blood vessels in retina absorb it much faster than the rest of the portions of the eye tissue. The reflected light is subsequently captured by the scanning device for processing.

Process of retina scanning involves image acquisition and processing, matching and representation of it in templete form. The size of templete is used to be very small (usually 96 bytes) which is smallest among other biometrics techniques.

Retina scans require that the person removes their glasses, place their eye close to the scanner, stare at a specific point, and remain still, and focus on a specified location for
approximately 10 to 15 seconds while the scan is completed[5].

6. Hand VeinPattern Recognition

Vein recognition systems mainly focus on the vascular patterns in the users hands. Compared to the other biometric systems, the user's veins are located inside the human body so difficult to duplicate, so vein authentication technology offers high level of accuracy.

Fig.9. Hand Vascular Pattern

Near-infrared rays from a bank of light emitting diodes penetrate the skin of the hand and produce an image caused by the absorbance of blood vessels. This image is digitized to prepare different templates, which forms the database of the biometric device. Various features used for templates are vessel branching points, thickness of veins and branching angles. The vascular imaging devices can be formed in either contacting type or to operate in a non-contact fashion. Non contacting method offers the benefit in that it is not necessary for the individual to touch the sensor to provide the biometric data. This is advantageous in applications where a high degree of hygiene is to be maintained, such as medical operating room access or where persons are sensitive about touching a biometric sensing device[6].

III. BEHAVIORAL TRAITS

1. Dynamic Signature Recognition

Signatures of individuals are used in day to day activities for authorizing financial transactions, documents, contracts etc. in this process the primary focus is used to be on the visual appearance of the signature. It can be regarded as simple signature comparison. For dynamic signature recognition, users write their signature on a digital tablet which is normally connected to a personal computer for processing and verification, thus real time acquisition of signature can be done[22]. The behavioral patterns inherent to the process of signing. includes the involved timing, pressure exerted while writing, and speed. Although it is comparatively simple to duplicate the visual appearance of a signature, it is very difficult to duplicate behavioral characteristics. The dynamic information used for recognition purpose usually consists of spatial coordinate x, spatial coordinate y, pressure p, azimuth az, inclination in, velocity v, acceleration a. this data is used for comparison purpose.

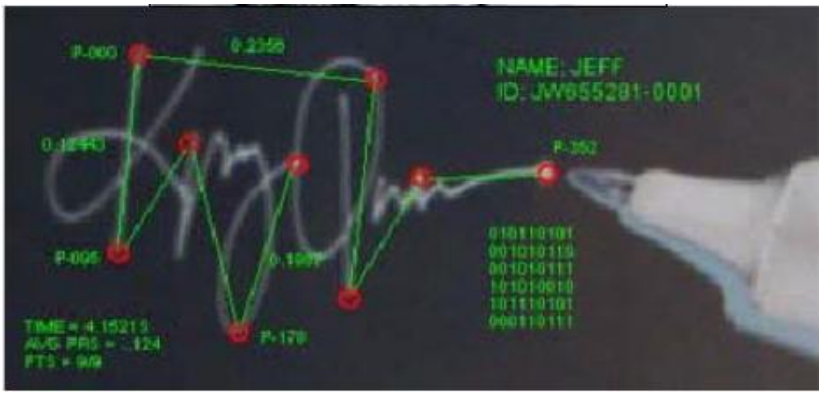

Fig.10. Information Extraction for Signature Recognition

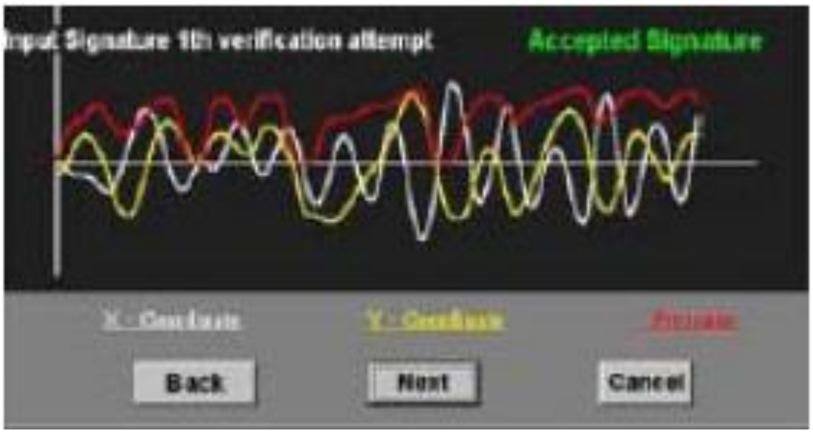

Fig.11. Signature Recognition

The most significant benefit of Signature Recognition is that it is highly resistant to impostors, as it is quite easy to forge a signature, but it is very difficult to ‘mimic’ the behavioral patterns inherent to the process of signing. On the other hand, Signature Recognition is prone to higher error rates, particularly when the behavioral characteristics of signatures are mutually inconsistent.

2. Voice Recognition

A person’s voice can be considered as one of the biometric trait because of two reasons. First the voice is actually the result of functioning of the physiological component which is known as the voice tract. Further it is a behavioral trait which is known as the voice accent. By combining these two factors, it is almost not possible to imitate another person's voice exactly. Voice recognition is a technology by which sound (words or phrases spoken by humans) are converted into electrical signals. These signals are transformed in to coded patterns for authentication purpose. The words or phrases are captured with the help of microphone. Input voice samples and enrolled models are compared to produce the likelihood ratio.

Fig.12. Voice Signal Captured by sensor

Voice changes because of aging also need to be considered by recognition systems. Further unauthorized users can record authorized users' voices and run it through the verification process in order to get user access control to system. To avoid the chances of unauthorized access with the help of recording devices, voice recognition systems will ask users to repeat various random phrases which are provided by the system during verification process.

IV. FACTORS OF EVALUATION

As presented in previous section, a variety of biometric authentication techniques are proposed by various researchers. The degree of security is one of the main concerns while evaluating a particular technique. Various parameters are there with which the performance of technique can be measured. Cross Error Rate(CER), False Accept Rate(FAR), False Reject Rate(FRR), Detection Error Tradeoff(DET), Failure to Enroll Rate(FTE), Failure to Capture Rate(FTC) are some of the commonly used factors.

V. CONCLUSION

Biometrics technology for authentication is a new technology as it has only been implemented in public for commercial purpose since a small period of time. There are many applications of biometrics technology specially in security systems. It provides accurate solution for recognition and detection problems. It has many advantageous features which can improve human living, such as improved security, effective authentication, reduced fraud, easy to use and implement. Further the cost of password administrator or token generator is saved. On the other hand biometrics security system still has many concerns to be dealt with, such as information privacy, physical privacy and religious objections. With all this it can be concluded that we can not deny the fact that this new technology will make our life comfortable and change it for the better.

VI. ACKNOWLEDGEMENT

Authors acknowledge Department of Instrumentation and Control Engineering, Faculty of Technology, Dharmsinh Desai University, Nadiad for providing resources and extending support.

REFERENCES

[1] Debnath Bhattacharyya, Rahul Ranjan, FarkhodAlisherov A., and Minkyu Choi, “Biometric Authentication: A Review” , International Journal of u- and e- Service, Science and Technology,Vol. 2, No. 3, September, 2009, pp. 13-28

[2] Dr.S.B.Thorat, S.K.Nayak, Miss.Jyoti P Dandale, “Facial Recognition Technology: An analysis with scope in India”, (IJCSIS) International Journal of Computer Science and Information Security,Vol. 8, No. 1, 2010, pp. 325-330

[3] Mohinder Pal Joshi, R.S. Uppal, Livjeet Kaur, “Development of Vision Based Iris Recognition System”, Mohinder Pal Joshi*et al. / (IJAEST) International Journal Of Advanced Engineering Sciences And Technologies Vol No. 6, Issue No. 2, pp. 277 – 281

[4] Alberto de-Santos-Sierr, Carmen Sa´nchez-A´ vila, Gonzalo Bailador del Pozo Javier Guerra-Casanova, “Unconstrained and Contactless Hand Geometry Biometrics”, Sensors 2011, 11, 10143-10164; doi:10.3390/s111110143 ISSN 1424-8220, www.mdpi.com/journal/sensors Article, Published: 25 October 2011

[5] András Róka, Ádám Csapó, Barna Reskó, Péter Baranyi, “Edge Detection Model Based on Involuntary Eye Movements of the Eye-Retina System”, Acta Polytechnica Hungarica Vol. 4, No. 1, 2007, pp.31
[6] E.Sridevi, B.Aruna, P. Sowjanya, “An Exploration of Vascular Biometrics” IJECT (International Journal of Electronics & Communication Technology)Vol. 2, SP-1, Dec . 2011,ISSN : 2230-7109(Online) | ISSN : 2230-9543(Print) IJECT Vol. 2, SP-1, Dec . 2011 , pp.181-184
[7] PalmSecure.http://www.fujitsu.com/us/services/biometrics/palm-vein
[8] http://fingerprint.nist.gov/latent/elft07/.
[9] Ross A, Nandakumar K, Jain AK (2006) Handbook of Multibiometrics. Springer.
[10] Sharath Pankanti, Salil Prabhakar, Anil K. Jain, "On the Individuality of Fingerprints," IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 24, no. 8, pp. 1010-1025, Aug. 2002, doi:10.1109/TPAMI.2002.
[11] Jain AK, Flynn PJ and Ross A (eds.) (2007) Handbook of Biometrics, Springer
[12] Jain, A.K.; Ross, A.; Pankanti, S, “Biometrics: a tool for information security” Information Forensics and Security, IEEE Transactions on Volume: 1 , Issue: 2 Digital Object Identifier: 10.1109/ TIFS.2006.873653 Publication Year: 2006 , Page(s): 125 – 143
[13] Anil K. Jain, Ajay Kuma, “ Biometrics of Next Generation: An Overview” appear in ‘second generation biometrics’ springer, 2010
[14] Samuel P. Fenker, Kevin W. Bowyer, “Analysis of Template Aging in Iris Biometrics”, Presented at IEEE Computer Society Biometrics Workshop, June 17, 2012
[15] Kalpana Saini, M.L.Dewal, “Designing of a Virtual System with Fingerprint Security by considering many Security threats”, International Journal of Computer Applications (0975 – 8887), Volume 3 – No.2, June 2010, pp.25-31
[16] Samuel P. Fenker, Kevin W. Bowyer, “Analysis of Template Aging in Iris Biometrics”, Presented at IEEE Computer Society Biometrics Workshop, June 17, 2012.
[17] M.Suganthy, P.Ramamoorthy, R.Krishnamoorthy, “Effective Iris Recognition For Security Enhancement”, International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622 www.ijera.com Vol. 2, Issue 2, Mar-Apr 2012, pp.1016-1019
[18] Craig Fancourt, Luca Bogoni, “Iris Recognition at a distance” AVBPA 2005, Vol. 3546: 1-13. Springer-Verlag, Berlin Heidelberg, 2005
[19] Ajay Kumar, David C. M. Wong, Helen C. Shen, Anil K. Jain , “Personal Verification using Palmprint and Hand Geometry Biometric”, Appeared in Proc. of 2nd Int'l Conference on Audio- and Video-based Biometric Person Authentication (AVBPA), Washington D.C., pp.166-171, March 22-24, 1999.
[20] Michael Brockly, James Scott, Richard Guest, Stephen Elliott, “Dynamic Signature Verifi cation and the Human Biometric Sensor Interaction Model”, 45th annual IEEE International Carnahan Conference on Security Technology, 253978-1-4577-0903-6/11/$26.00 ©2011 IEEE
[21] Simarpreet Kaur, Purnima, “Speaker Verification using LabVIEW”, International Journal of Computer Applications (0975 – 8887), Volume 21– No.4, May 201, pp.31-38
[22] www.Biometrics.gov

BIOGRAPHY

1. **Prof.Shweta Gaur**: She completed B.E. (Electronic Instrumentation and Control Engineering) from University of Rajasthan. She is having an industrial experience of 4.5 years and teaching experience of 4 years. She is pursuing M.Tech(Instrumentation and Control Engineering) from DharmSinh Desai University, Nadiad. Her areas of interests are PLC, SCADA, DCS, LABVIEW.

2. **Prof.(Dr.)V.A.Shah**: He is Ph.D.in Instrumentation and Control Engineering. He is working as Head of deptt.(Instrumentation and Control Engineering), DharmSinh Desai University, Nadiad. He is having an industrial experience of 2 years and teaching experience of 16 years. He is having 25 papers published in national journals. He also has six international publications. His areas of interest are Neural Network & Fuzzy Logic, Microprocessors & Microcontrollers, Robotics, System Design.

3. **Prof.Manish Thakker**: He completed M.E. (Instrumentation and Control Engineering) from DharmSinh Desai University, Nadiad, and pursuing PhD. He is having a teaching experience of 10 years. His areas of interest are virtual instrumentation, surface science and technology.