# Personal Identification Using Different Biometrics : A Review

[1.]Santosh P. Shrikhande, [2.]Hanumant S. Fadewar
[1.]Assistant Professor, School of Technology, SRTM, University, Sub-Centre, Latur
[2.]Assistant Professor, School of Computational Sciences SRTM, University, Nanded

**Abstract— Biometrics is the method of automatic identification of an individual by using their certain measurable physiological or behavioral characteristics like fingerprints, palm prints, hand geometry, iris, retinas, faces, hand veins, facial expressions, signatures, and voiceprints. Biometrics has overcome the problems of traditional verification methods like cards, tokens and Password or PINs. Biometric indicators have an edge over traditional security methods in that these attributes cannot be easily forgotten, stolen or shared; personally they have to go through the system. This paper reviews all biometrics and their various studies that have explored the technical and convenience issues and comparison between all the biometrics with an objective to provide insights on their reliability, performance, security, convenience and acceptance.**

**Keywords: Biometrics, verification, authentication**

## I. INTRODUCTION

Now a day's world is becoming very much insecure and hence people are looking towards the new type of security which is more secure, reliable and accurate. Biometric is one of them recent technology which provides reliability, security and accuracy [3]. Biometric is the technology of verifying people by using their measurable physiological or behavioral characteristics such as finger print, palm print, faces, retinas, iris, voice, and gait [4, 26]. Biometric authentication is highly reliable, because they provide a nontransferable method of identifying people and not just cards, badges or keys [2]. The main advantage of using biometrics is that human characteristics cannot be misplaced or forgotten like cards, password or PINs. Biometrics characteristics are classified into two categories.

### *A.* Physiological Characteristics

The characteristics those are related to the human body or body shapes those are varies from person to person like Finger print, Palm print, Hand geometry, Hand veins, Face, Iris, Retinas and etc [1, 2, 26].

### *B.* Behavioral Characteristics

The characteristics those are related to behavior of person while doing some actions such as Signatures, voice, Gestures, Gait, Keystrokes, Facial expressions and etc [1, 2, 26].

## II. BIOMETRIC SYSTEMS

Biometric systems are the automated systems can automatically recognize the person on the basis of their physiological and behavioral characteristics [4]. Biometric systems involve following units through which recognition is done which is shown in the following figure1.

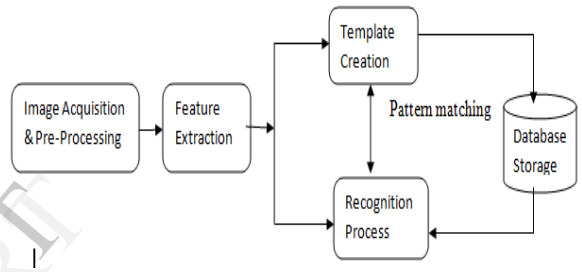


Figure 1: Biometric Recognition System

### *A. Acquisition Unit*

In acquisition unit an image is captured by the sensing device such as camera. This is the important unit because the accuracy of entire system is totally depending on the quality of input image. So better the quality of image acquisition, better the image recognition [3].

### *B. Preprocessing Unit*

In preprocessing unit the input image quality is enhanced by applying various preprocessing techniques for the better feature extraction purpose. Image preprocessing involves removing low frequency backgrounds, noise, normalizing the intensity of each pixel and image transformations [3, 5].

### *C. Feature extraction Unit*

Introducing images to the computer system is called as feature extraction. In this unit image features are extracted those can be used to identify the person based on fact that each person has unique characteristics. For example finger print of person has the features like whorls, arches, loops, ridges, furrows and minutiae. There are many more features extraction techniques and algorithms are used to extract the features from biometric trait. The extracted features are represented as a vector called as features vector which is useful in matching unit [3, 5].

### *D. Matching Unit*

In the Matching unit, the features of query image are compared with the template image features. If the query image features are matched with template image then recognition is successful. This process can be done in two

steps - Verification stage or Identification stage. In verification stage, it has to verify the person who claims an identity. So his biometric features those were extracted are compared with the stored trait in the database. Actually this is a one to one matching process. But in the identification process the extracted features are compared with all the features those are stored in the database. So the identification process is a one to many matching process [3, 5].

## III. BIOMETRICS TYPES

Based on Physiological and behavioral Characteristics following are the biometric types [1] discussed in this paper.

### *A. Finger Print Technology*

This is the oldest of all biometric technique and widely accepted by the people. Its applications are in forensic investigation, law enforcement, personal identification and end point security. Finger print is an impression of the ridges of all parts of the finger [2, 5]. The fingerprint image contain dark lines are called as ridges and bright lines are called as valleys. Ridges and valleys run parallel, sometimes they bifurcate or sometime joins in one or sometime they terminates. The points where the ridges are suddenly terminated or bifurcated or combined such points are called as minutiae points [21]. A good quality finger print containing around 25-80 numbers of minutiae point. Based on the ridge valley pattern, finger print matching techniques can be classified as minutiae based or correlation based. Minutiae based techniques attempts to match minutiae points of query image with template image and determine the total number of matched minutiae. Correlation based technique compares the global pattern of ridges and furrows to see if the ridges in the two finger prints are matching or not [2, 21].

### *B. Face Recognition Technology*

Face recognition is the automated method of detecting and matching a face of person with existing database [2, 9]. Face recognition technologies are used in airports, multiplexes, malls and other public places to detect the presence of criminals, terrorist among the public crowd [6]. Every human face has unique and distinct landmarks and these landmarks are called as Nodal points. Human face has around 80 nodal points. In face features extraction, most of the techniques analyzes the relative position of the face, size of the face, shape and depth of the eyes, distance between the two eyes, size and shape of nose, nasal breadth, cheek boons and depth of jaw line of the person's face [3, 7, 21]. These features are stored in feature vector and used for verification and identification purpose in matching step of the face recognition system [2, 3]. Face recognition system uses different approaches for the recognition; Holistic approach method uses whole face image for feature extraction is commonly called appearance based strategy. The feature based method uses local features of the face such as nose, mouth, eyes, eyebrows and their relationship with each other. The Hybrid approach method uses combination of both holistic and feature based method for better performance [8]. There are two types of face recognition systems, first is 2-D system, which require more illumination to capture an image and supports minor variations in the face orientation. Hence it is very difficult to recognize the face with expressions and orientation [6, 7]. Second is 3-D system, where range cameras are used to capture the 3-D view of faces. This system supports variations in faces orientation up to 90 degree and hence it is not so difficult to recognize the facial expression and orientation [6, 7, 8].

### *C. Iris Recognition Technology*

Iris recognition system uses an iris of human eye which is unique in every individual [5]. Iris recognition is used in various areas of life such as airports, crime detection, business applications, banks, and personal identification in firms and industries. Iris recognition is becoming an important biometric as compare to other because iris is protected from external environment behind the cornea and the eyelid [2]. Iris is the annular colored ring between the pupil and sclera of the eye and structure of iris is fixed over a time. The gray level intensities of iris of two individuals differs from each other. This difference is found in between identical twins and even in between left and right eye of the same person [9]. Iris image is captured by the camera with proper illumination for the better quality of iris image. Preprocessing techniques are applied on iris image for better feature extraction purpose such as pupil and iris boundary, eyelid detection and its removal [9]. Feature extraction module extracts the most significant features of an iris for the verification and recognition purpose. Some of the feature extraction techniques of iris are based on the radius of iris, orientation of pupil, shape and size of the pupil, intensity values of pupil and ratio of average intensity values of the two pupils [9]. Matching module compares the features of input iris image with the stored template iris image features [2, 9].

### *D. Voice Recognition Technology*

The voice recognition biometric uses the voice of human being for identification. Voice is a very basic means for communication amongst the people [12]. It is also called as speech recognition system. Speech recognition is a process of converting speech signals to the words by means of algorithms and hence it is the special form of signal processing [5]. Automatic speech recognition has a wide range of application in such a areas where human interface is not required such as automatic call processing in telephone network, telephone directory inquiry without operator help, ovens, refrigerators and washing machine, robotics, automated transcription, and air traffic control [11]. Speech recognition system is divided in four different categories based on the type of utterance they can identify [11, 12]. First is Isolated word, where each utterance should quiet on both sides of sample window hence it accepts single word or utterance at a time. Second is Connected word, where it will allow separate utterance to be run together minimum pause between them. Third is continues speech, it will allow the user to speak naturally continuous while computer determine the contents. Fourth is Spontaneous, where it will allow natural sounding and not rehearsed such as words like run together, "ums" and "ahs". The different feature extraction techniques used in speech

recognition are Spectral features such as band energies, formats, spectrum and Cepstral coefficient mainly speaker specific information due to vocal tract, Excitation source feature such as pitch and variation in pitch, Long term feature such as duration, information energy due to behavior feature [11].

### *E. Finger Vein Recognition Technology*

One of the recent biometric recognition technology invented is vein recognition. Finger vein authentication biometric uses the vein pattern of individual's finger for their personal identification. Every individual has a different vascular vein pattern in his finger which circulates the blood towards heart [15, 20]. Finger vein authentication is a promising biometric for individual identification in terms of reliability, security and convenience that is why many more applications are using finger veins authentication [17]. This biometric is reliable, secure, accurate and efficient as compare to other biometrics because of following reasons [17, 20].

- Veins pattern is hidden inside the body skin and hence invisible to human eyes so it is difficult to forge.
- It is contactless hence it is hygienic and more acceptable by the people.
- Finger veins pattern image can only be taken from live body hence dead body cannot be used for identification.
- Finger veins pattern is different even among identical twins and remain constant through the adult years. Hence it provides high accuracy [20, 26].

Finger vein authentication process is done in four steps. The finger vein image is captured using near infrared camera. When infrared light passes on the finger then hemoglobin in the blood veins absorbs the penetrated infrared light and reflects vein image as the darker lines [15, 17, 20]. In preprocessing stage various techniques are used for vein image pattern adjustment and enhancement. In feature extraction module the measurable characteristics, attributes are used for introducing finger vein image to the computer systems for their recognition. In matching module the extracted features of input image is compared with template image for the recognition [20, 26].

### *F. Some other biometrics*

Some of the other biometrics based on individual's physiological and behavioral characteristics are discussed below.

- Hand Geometry

Hand geometry biometric uses hand measurement characteristics of human for recognition purpose based on the fact that every human has unique hand geometry [2]. Hand measurement characteristics are length, width, thickness of the fingers, aspect ratio of the palm or fingers, thickness of the hand, curvature and relative location of these features differentiate every human. This biometric provide less accuracy in recognition because hand shape changes as per the age but it has a great user acceptance due to its ease of use and cost [3, 23].

- Retina Recognition

Retina scan biometric uses retina of the human being for recognition purpose as every individual has a unique retina. The structure of the retina includes sensing tissues and image receptor elements called as cones and rods. These cons and rods accept light rays and send the electrical impulses to brain for forming an image. Retina is not directly being seen so infrared light is used to illuminate the retina. The blood veins in the retina absorb infrared light and produce an image where blood veins appears as a dark lines. This retina blood veins pattern is used for the recognition. This biometric is very much accurate in terms of reliability and accuracy due to its uniqueness but very poor in terms of hardware cost and user acceptance [3, 24].

- Signature recognition

Signature recognition technology recognizes the person based on their behavioral signature. The signature of an individual is taken by the special pen and writing pad which is connected to the computer. While doing signature this system extracts the information of signature features based on the behavioral characteristics like speed, overall size, directions, acceleration, length of stroke and their time duration. These extracted features are stored as a template which is useful for person recognition. The advantage of this system is that it is easy to use and widely accepted by the people but it is less secure and accurate in terms of recognition [2, 3].

- Keystroke Recognition

Keystroke recognition technology uses the behavior of person while typing on the keyboard based on the fact that each individual has unique behavior. This technology contains keyboard connected to the computer and user is suppose to type. When user starts typing it extracts the behavioral features like the way person types, cumulative typing speed, time that elapses between the strokes, time that each key is held down. These features are used to recognize the person uniquely. Keystroke recognition is widely used due its ease of use and low cost but it provides less accuracy in recognition [2, 25].

- DNA Recognition

DNA recognition biometric recognizes the person based on the DNA sample as every person has unique DNA pattern. DNA is made-up of the "nucleotides" and it can be taken from blood, semen, tissues, cells and urine of the human being. The DNA samples from above sources are used for the recognition of an individual. This biometric used in forensic for crime detection and also used to prove the blood relations with parents. This biometric provide a great accuracy and reliability in recognition but has a very less user acceptance due to the implementation cost [2, 3, 5].

## IV. EVALUATION OF BIOMETRICS

Nowadays it is well accepted that biometrics will never produce an error free recognition results. Therefore for the better use of any biometric system it has to evaluate for their

performance, reliability and security based on following parameters [3, 18, 20].

### *A. Security*

Biometrics is used for the secure identification and hence Security is the most important factor in evaluating the biometric systems. The security is referred as how secure and stable the biometric trait against anti forgery and permanence [3].

- Anti forgery

The data input can be forged or illegally used the trait of person for authentication such as the finger print on the glass can be used for authentication [20].

- Permanence

How much this Biometric trait is stable and it does not change over a time hence continue to work without data updates over long periods of time. This is also called as Long Term Stability of trait.

### *B. Accuracy and Reliability*

Accuracy and reliability are the very much important factors that need to be considered while evaluating any biometric authentication system. Reliability is the rate of dependability on biometric for recognition purpose. Accuracy is the rate of correctness in recognition and which is measured using following factors [3].

- False Accept Rate (FAR)

The probability of accepting an imposter individual as a valid individual is called as False Acceptance Rate (FAR). It measures the rate of invalid matches, Less the FAR rate, better the authentication accuracy and reliability [3, 19].

- False Rejection Rate (FRR)

The false rejection rate is the percentage of rejecting the valid individual who is genuine user to the system. Less the FRR rate, better the authentication accuracy and reliability [19].

- Equal Error Rate (EER)

Equal Error Rate is the percentage of both accepting and rejecting rate is equal. The EER is obtained by taking the point where FAR and FRR is having same value. The lower is the EER; higher accuracy is considered [19].

- Failure to Enroll Rate (FER)

The rate at which biometric system fails to enroll the captured input image in a system by the acquisition unit. This is called as Failure to Enroll Rate (FER) where input accepted by sensor is treated as invalid input [19].

### *C. Practicality*

Practicality is the major parameter to be considered while designing and implementing the biometric recognition system. It is measured based on the following aspects [20].

- Performance

The Performance or the speed of the biometric authentication system is that how quickly it gives the response to the users and does verification and identification [3].

- Convenience

Convenience is referred as how easily and simply one can use the biometric trait and the biometric system for recognition. This is also called as the ease of use where user can easily use the biometric system for recognition. If the biometric system is more convenient and easy to use then user acceptance is more to that system [3, 20, 27].

- Hardware Cost

Cost of the biometric system affects performance and security of authentication. The hardware cost is the cost requires to designing and implementing the biometric recognition system. Low-cost biometric doesn't provide high level of security. An ideal biometric will be "cost-effective", when it is capable to provide a relatively high level of security at a low cost [3].

- Template Size

Size of sensing device is depending on the size of biometric trait used for the recognition. The size required to store the biometric trait into the database is called as template [3, 27]. The template size is depending on the size and quality of input data that will be stored in to the database.

## V. COMPARISON OF ALL BIOMETRICS

The biometric systems are evaluated on the basis of above all factors and their comparison is done on the basis of evaluated performance factors. The ideal biometric is one which rarely rejects an authorized individual (low false rejection rate, FRR) and rarely accepts an unauthorized individual (low false acceptance rate, FAR). The comparison of major biometrics based on the factors such as anti forgery, accuracy, reliability, long term stability, error rate, ease of use, user acceptance and hardware cost is shown in the following Table 1. [3, 20, 27].

Table 1: Biometrics Comparison Chart

| Biometric Type | Anti Forgery | Accuracy | Reliability | Long Term Stability | Error Rate | Ease of Use | User Acceptance | Hardware Cost | Errors Due to |
|---|---|---|---|---|---|---|---|---|---|
| Finger Print | Low | High | High | High | 1 in 500+ | High | Medium | Low | Dryness, age, dirt. |
| Face Prints | Medium | Medium | Medium | Medium | No data | Medium | Medium | Low | Age, glasses, hairs. |
| Hand Geometry | Medium | Medium | Medium | Medium | 1 in 500 | High | Medium | High | Age, hand injury. |
| Speech / Voice | Medium | Low | Low | Medium | 1 in 50 | High | High | Low | Noise, weather, cold. |
| Iris Scan | Medium | Very High | High | High | 1 in 1,31,000 | Medium | Medium | High | Poor light, eye diseases. |
| Retina Scan | High | Very High | High | High | 1 in 10,000, ,000 | Low | Medium | High | Poor lightning, eye diseases. |
| Signature | Medium | Low | Low | Medium | 1 in 50 | High | Medium | Low | Change in signatures. |
| Keystroke | Medium | Very Low | Low | Low | No data | High | High | Low | Hand injury, Tiredness. |
| DNA | Medium | High | High | High | No data | Low | Low | High | None. |
| Veins Pattern | High | High | High | High | No data | Medium | Medium | Medium | None. |

A perfect and ideal biometric system is one which would be very good at all the factors given in the above Table1.

## VI. CONCLUSIONS

This paper has discussed different biometric systems with their techniques for the feature extraction and authentication process. This paper has attempted to provide a comprehensive survey of all biometric recognition methods and their comparison for their reliability, performance, security, convenience, and user acceptance. This review has found that Iris and Retina recognition biometrics are more accurate in terms of recognition but they are poor in terms of practicality due to special hardware's cost and user acceptance due to the rays those are used for capturing iris scan are harmful to the eyes. Second is DNA recognition is also providing a great accuracy in recognition but it is very poor in practicality due to its practicality cost. Overall, the finger vein biometric is more secure and good in terms of anti forgery, accuracy and speed as well as average in terms of convenience and practicality. Hence Finger vein biometric is the promising, challenging and more acceptable biometric for personal identification. It is also found that unimodal biometric system is not enough for recognition accuracy purpose therefore multimodal biometrics can be used for the better security and accuracy results. We hope this review paper helps the researchers to choose their appropriate biometric trait for research among above biometrics or can go for multimodal biometrics.



## REFERENCES

[1] Fahad Al-harby, Rami Qahwaji, and Mumtaz Kamala, "Secure Biometrics Authentication: A brief review of the Literature"
[2] Debnath Bhattacharyya, Rahul Ranjan, Farkhod Alisherov A., and Minkyu Choi, "Biometric Authentication: A Review", *International Journal of u- and e- Service, Science and Technology*,Vol. 2, No. 3, September, 2009
[3] Nimalan Solayappan and Shahram Latifi, "A Survey of Unimodal Biometric Methods"
[4] Sakshi Goel, Akhil Kaushik, Kirtika Goel, "A Review Paper on Biometrics: Facial Recognition", *International Journal of Scientific Research Engineering & Technology (IJSRET)*, ISSN 2278 – 0882, Volume 1 Issue 5 pp 012-017 August 2012
[5] Sourav Ganguly, Subhayan Roy Moulick, "A Review On Different Biometric Techniques", *International Journal of Engineering Research & Technology (IJERT)*, ISSN: 2278-0181, Vol. 1 Issue 5, July – 2012
[6] Akazue M and Efozia N. F, "A Review Of Biometric Techniques For Securing Corporate Stored Data", *Proceedings of the International Conference on Software Engineering and Intelligent Systems 2010*, July 5th-9th, Ota, Nigeria SEIS 2010.
[7] Andrea F. Abate, Michele Nappi, Daniel Riccio, Gabriele Sabatino, " 2D and 3D face recognition: A survey", *Science Direct, Pattern Recognition Letters* 28 (2007) 1885–1906
[8] Patil A.M, Kolhe S.R and Patil P.M, "2D Face Recognition Techniques: A Survey", *International Journal of Machine Intelligence*, ISSN: 0975–2927, Volume 2, Issue 1, 2010, pp-74-83
[9] S V Sheela, P A Vijaya, "Iris Recognition Methods – Survey", *International Journal of Computer Applications* (0975 – 8887), Volume 3 – No.5, June 2010
[10] Mansi Jhamb, Vinod Kumar Khera, "IRIS Based Human Recognition System*", International Journal of Biometrics and Bioinformatics (IJBB)*, Volume (5) Issue (1) : 2011
[11] M.A.Anusuya, S.K. Katti, "Speech Recognition by Machine: A Review", *International Journal of Computer Science and Information Security*, Vol. 6, No. 3, 2009
[12] Santosh K.Gaikwad, Bharti W.Gawali, Pravin Yannawar, "A Review on Speech Recognition Technique", *International Journal of Computer Applications* (0975 – 8887), Volume 10– No.3, November 2010
[13] Shanthi Therese, Chelpa Lingam, "Review of Feature Extraction Techniques in Automatic Speech Recognition", *International Journal*

*of Scientific Engineering and Technology* (ISSN : 2277-1581), Volume No.2, Issue No.6, pp : 479-484 1 June 2013

[14] Bhupinder Singh, Rupinder Kaur, Nidhi Devgun, Ramandeep Kaur, "The process of Feature Extraction in Automatic Speech Recognition System for Computer Machine Interaction with Humans: A Review", *International Journal of Advanced Research in Computer Science and Software Engineering*, Volume 2, Issue 2, February 2012 ISSN: 2277 128X

[15] Naoto Miura, Akio Nagasaka, Takafumi Miyatake, " Feature extraction of finger-vein patterns based on repeated line tracking and its application to personal identification", *Machine Vision and Applications* (2004) 15: 194–203, Digital Object Identifier (DOI) 10.1007/s00138-004-0149-2, Published online: 21 July 2004 –_c Springer-Verlag 2004

[16] Naoto Miura, Akio Nagasaka, Takafumi Miyatake, "Extraction of Finger-Vein Patterns Using Maximum Curvature Points in Image Profiles", MVA2005 *IAPR Conference on Machine VIsion Applications*, May 16-18, 2005 Tsukuba Science City, Japan

[17] T. Prasanth, R .Praveen Chandran, B.Vigneshwaran, "Biometric Based Finger-vein recognition For Automatic Teller Machine", *International Journal of Research in Engineering & Advanced Technology (IJREAT)*, Volume 1, Issue 1, March, 2013 ISSN: 2320 – 8791

[18] Dmitry O. Gorodnichy, "Evolution and evaluation of biometric systems", *IEEE Symposium on Computation Intelligence for Security and Defence Applications* (CISDA'09)

[19] Hitachi Finger Vein Authentication: Frequently Asked Questions ( FAQ) , 2006

[20] Ben Edgington, "Introducing Hitachi's Finger Vein Technology: A White Paper", May 2007

[21] Ms.Poonam Mote, Prof.P.H.Zope, Prof. S. R. Suralkar, "Finger And Face Recognition Biometric System", *International Journal of Scientific & Engineering Research* Volume 3, Issue 10, October-2012 1 ISSN 2229-5518

[22] Pranoti Das, Sachin Meshram, "An Efficient Hand-Geometry System for Biometric Identifications", *Journal of Electronics and Communication Engineering (IOSR-JECE)* ISSN: 2278-2834, ISBN: 2278-8735. Volume 4, Issue 4 (Jan. - Feb. 2013), PP 17-19

[23] Dewi Yanti Liliana, Eries Tri Utaminingsih, "The combination of palm print and hand geometry for biometrics palm recognition", *International Journal of Video & Image Processing and Network Security IJVIPNS-IJENS* Vol: 12 No: 01

[24] Delia Cabrera Fernández, Harry M. Salinas, Carmen A. Puliafito, "Automated detection of retinal layer structures on optical coherence tomography images", (100.5010) *Pattern recognition and feature extraction;* (100.2980) Image enhancement; (110.4500) Optical coherence tomography.

[25] Arwa Alsultan and Kevin Warwick, "Keystroke Dynamics Authentication: A Survey of Free-text Methods", *International Journal of Computer Science Issues(IJCSI)*, Vol. 10, Issue 4, No 1, July 2013 ISSN (Print): 1694-0814 | ISSN(Online):1694-0784.

[26] T.Sheeba, M.Justin Bernard, "Survey on Multimodal Biometric Authentication Combining Fingerprint and Finger vein", *International Journal of Computer Applications (0975 – 8887) Volume 51– No.5, August 2012*

[27] K P Tripathi, "A Comparative Study of Biometric Technologies with Reference to Human Interface", *International Journal of Computer Applications (0975 – 8887) Volume 14– No.5, January 2011*