International Journal of Engineering Science Invention
ISSN (Online): 2319 – 6734, ISSN (Print): 2319 – 6726
www.ijesi.org Volume 3 Issue 6‖ June 2014 ‖ PP.24-30

Biometric Technology: A Look and Survey at Face Recogntion

Urvashi Bakshi[1] Rohit Singhal[2] Monika Malhotra[3]

[1] *Asst. Professor, Computer Science Deptt. World College of Technology and Management, Gurgaon.Haryana.*
[2] *Associate Professor, Computer Science Deptt. Institute of Engineering and Technology, Alwar, Rajashtan.*
[3] *Asst. Professor, Computer Science Deptt. World College of Technology and Management, Gurgaon, Haryana.*

ABSTRACT: *Biometrics is the science and technology of measuring and analyzing biological data. It is used to uniquely identify individuals by their physical characteristics or personal behaviour traits. Biometrics" means "life measurement" but the term is usually associated with the use of unique physiological characteristics to identify an individual. The application which most people associate with biometrics is security. A number of biometric traits have been developed and are used to authenticate the persons identity. In this paper various biometric techniques are discussed, special focus on facial recognition system and its advantages over other biometric techniques.*

KEYWORDS: *Biometrics, face recognition*

I. INTRODUCTION

The method of identification based on biometric characteristics is preferred over traditional passwords and PIN based methods for various reasons such as: The person to be identified is required to be physically present at the time-of-identification. Identification based on biometric techniques obviates the need to remember a password or carry a token. Biometric technologies are thus defined as the "automated methods of identifying or authenticating the identity of a living person based on a physiological or behavioral characteristic". [4] A biometric system is essentially a pattern recognition system that operates by acquiring biometric data from an individual extracting a feature set from the acquired data, and comparing this feature set against context, a biometric system may operate either in verification mode or identification mode.

- **Verification** mode: in verification mode, the system validates a person's identity by comparing the captured biometric data with her/his own biometric template(s) stored in the system database. In such system, an individual who desires to be recognized claims an identity, usually via a personal identification number (PIN), a user name, or a smart card, and the system conducts a one to one comparison to determine whether the claim is true or not (e.g."Does this biometric data belong to Mr. X?"). Identify verification is typically used for positive recognition, where the aim is to prevent multiple people from using the same identity [12]
- **Identification** mode: In identification mode, the system recognizes an individual by searching the templates of all the users in the database for a match. Therefore the system conducts a one to many comparison to establish an individual's identity (or fails if the subject is not enrolled in the system database)[12].

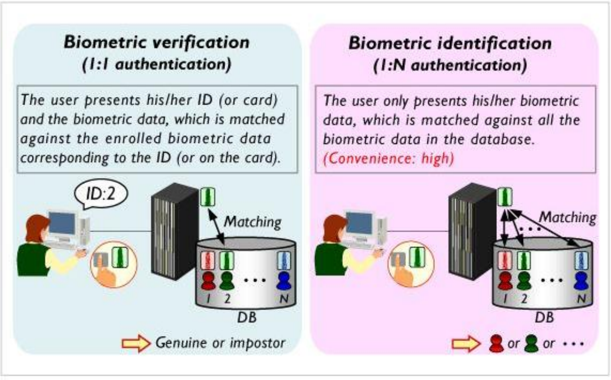
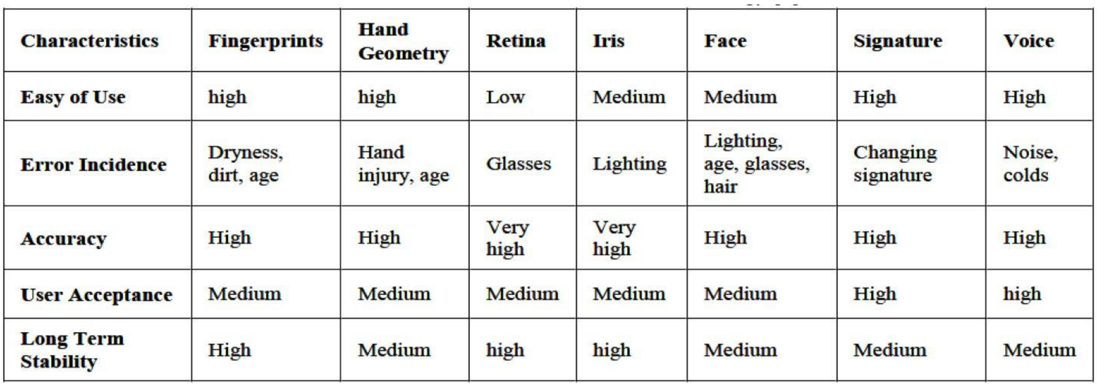

Biometric verification
(1:1 authentication)
The user presents his/her ID (or card) and the biometric data, which is matched against the enrolled biometric data corresponding to the ID (or on the card).
ID:2
Matching
1
2
N
DB
Genuine or impostor
Biometric identification
(1:N authentication)
The user only presents his/her biometric data, which is matched against all the biometric data in the database.
(Convenience: high)
Matching
1
2
N
DB
or
or

Figure 1. Biometric verification and Biometric Identification (in case of PC log-in) [5]

II. BIOMETRICS CHARACTERSTICS

“Biometrics” means “life measurement” but this term is generally couple with the use of unique and accurate physiological characteristics to identify a person, some characteristics of biometrics are:

[1] **Universal:** Every person must possess the characteristic/attribute. The attribute must be one that is universal and seldom lost to accident or disease.
[2] **Invariance of properties:** They should be constant over a long period of time. The attribute should not be subject to significant differences based on age either episodic or chronic disease.
[3] **Measurability:** The properties should be suitable for capture without waiting time and must be easy to gather the attribute data passively.
[4] **Singularity:** Each expression of the attribute must be unique to the individual. The characteristics should have sufficient unique properties to distinguish one person from any other.
[5] **Acceptance:** The capturing should be possible in a way acceptable to a large percentage of the population. Excluded are particularly invasive technologies, i.e. technologies which require a part of the human body to be taken or which (apparently) impair the human body.
[6] **Reducibility:** The captured data should be capable of being reduced to a file which is easy to handle.
[7] **Reliability and tamper-resistance:** The attribute should be impractical to mask or manipulate. The process should ensure high reliability and reproducibility.
[8] **Privacy:** The process should not violate the privacy of the person.
[9] **Comparable:** Should be able to reduce the attribute to a state that makes it digitally comparable to others. The less probabilistic the matching involved, the more authoritative the identification.
[10] **Inimitable:** The attribute must be irreproducible by other means. The less reproducible the attribute, the more likely it will be authoritative. [1]



Characteristics	Fingerprints	Hand Geometry	Retina	Iris	Face	Signature	Voice
Easy of Use	high	high	Low	Medium	Medium	High	High
Error Incidence	Dryness, dirt, age	Hand injury, age	Glasses	Lighting	Lighting, age, glasses, hair	Changing signature	Noise, colds
Accuracy	High	High	Very high	Very high	High	High	High
User Acceptance	Medium	Medium	Medium	Medium	Medium	High	high
Long Term Stability	High	Medium	high	high	Medium	Medium	Medium

TABLE 1. Characteristics features of Biometric technology [3]

III. VARIOUS BIOMETRIC TECHNOLOGIES

Biometric technologies are widely used in commercial, government and forensic application area and all these area acquire various biometric techniques. A number of various Biometric techniques exist and are in use in various applications. Each biometric has its strength and weakness. A brief introduction to some of the biometric techniques is given below and the images are shown in figure(2).

DNA: Deoxyribonucleic acid (DNA) is the one dimensional ultimate unique code for one’s individuality-except for the fact that identical twins have identical DNA patterns. It is however, currently used mostly in the context of forensic applications for person recognition. There is total three issues limit the utility of this biometric for other applications: 1) contamination and sensitivity, 2) automatic real time recognition issues and 3) privacy issues. [2]

EAR: The ear recognition approach is basically based on matching the distance of salient points of the pinna from a landmark location of the ear. The features of an ear are not expected to be very unique or distinctive in establishing the identity of an individual.

FACE: It is probably most common biometric characteristics use by humans to make personal recognition. The face recognition technology can be either static, controlled verification or it can be dynamic uncontrolled face identification method. The most famous approaches to face recognition are either based on (i) location and shape of eyes, eyebrows, lips, nose and chin or (ii) the global analysis of the face image that represents a face which is a combination of number of canonical faces.

FACIAL, HAND AND HAND VEIN THERMOGRAM: one important characterstic of an individual is the pattern of heat radiated by human body. This characterstic of a human can be captured by an infrared camera in an unobtrusive way much like a regular photograph. A thermogram base system will not require contact and is uniquely noninvasive.

FINGERPRINTS: The mode of fingerprinting technology for human identification is been used from many centuries and its matching accuracy is also very high. Fingerprints of an identical twins are always different and so are the prints on each finger of the same person.

GAIT: It is a unique way of walking of a human and it’s a spatio temporal biometric technique. It is not suppose to be very disticntive and hence used in low security application. It comes under behavioral biometric and gate based system uses video sequence footage of a person’s walking to measure several different movements.

HAND: Hand scan and recogntion is based on the measurements of the human hand such as, shape, length and width of the fingures, size of palm etc. The size of the hand geometry base system is quite large and thus can not be used in certain devices like laptops. Some of hand geometry scanners produce only the video signal with the hand shape. Image digitalization and processing is then done in the computer to process those signals in order to obtain required video or image of the hand [14, 16].

IRIS: The iris is the annular region of the eye bounded by the pupil and the sclera (white of the eye) on either side. The visual texture of the iris is formed during fetal development and stabilizes during the first two years of life. The accuracy and speed of currently deployed iris-based recognition systems is promising and point to the feasibility of large-scale identification systems based on iris information. Each iris is distinctive and, like fingerprints, even the irises of identical twins are different. [2]

RETINA: Retina scan is based on the blood vessel pattern in the retina of the eye. Retina scan technology is older than the iris scan technology that also uses a part of the eye. [6]. Retina is not directly visible and so a coherent infrared light source is necessary to illuminate the retina. The infrared energy is immersed more rapidly by blood yacht in the retina than by the surrounding tissue. The image of the retina blood vessel pattern is then analyzed for characteristic points within the pattern. The retina scan is more susceptible to some diseases than the iris scan, but such diseases are relatively rare [7].

PALM PRINT: The palms of the human hands contain pattern of ridges and valleys much like the fingerprints. The area of the palm is much larger than the area of a finger and, as a result, palmprints are expected to be even more distinctive than the fingerprints. Since palmprint scanners need to capture a large area, they are bulkier and more expensive than the fingerprint sensors[15].

SIGNATURE: It is process used to recognize a person’s hand written signature. It is a behavioral biometric and comes under dynamic verification technology. The technology uses the analysis of the speed, shape, stroke, and pen pressure and timing information during the act of signing naturally.

VOICE: Voice recognition technology does not measure the visual features of the human body. In voice recognition sound sensations of a person is measured and compared to an existing dataset. The person to be identified is usually required to speak a secret code, which facilitate the verification process [1].

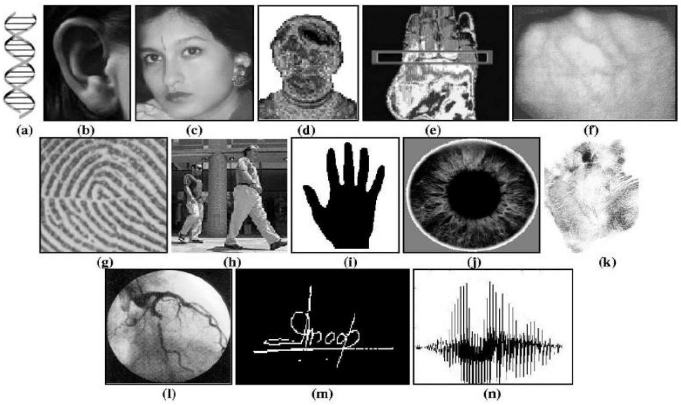


Figure2: examples of biometric characteristics: (a)DNA, (b) ear, (c) face, (d) facial thermogram (e) hand thermogram (f) hand vein (g) fingerprint (h) gait, (i) hand geometry, (j) iris (k) palm print, (l) retina, (m) signature, and (n) voice [2]

IV FACE RECOGNITION

(A) Overview:

Face recognition is an interesting application of pattern recognition and recently it has received significant attention. The task is can be done by matching a selected face to one of many faces present in the dataset. It is a most reliable method of biometric personal identification. Various techniques have been proposed and much work has been done in recognizing face under small variations in face orientation, expressions, lighting, back-ground [8]. Face recognition system can be used in various human -machine interfaces and various other automatic access control systems. It’s true challenge to build an automated system which equals human ability to recognize faces. Although humans are quite good identifying known faces, we are not very skilled when we must deal with a large amount of unknown faces. The computers, with an almost limitless memory and computational speed, should overcome human limitations. Face recognition remains as an unsolved problem and a demanded technology [10].

(B) Facial Recognition Technology (FRT)

Facial recognition technologies are basically divided into two areas and they are Facial metric and Eigen faces. Facial metric technology relies on the manufacture of the specific facial features that is the system usually look for the positioning of eyes, nose and mouth and distances between these features , shown in the following figures.

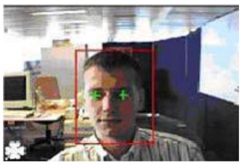


Figure 3: Recognition of face from body

The face region is rescaled to a fixed pre-defined size (e.g. 150-100 points or 180-200 points). This normalized face image will be called the canonical image. Then the facial metrics are computed and then stored in a face template. The figure for the normalized face is given below.

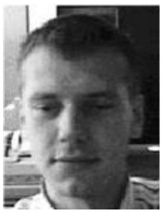


Figure 4: Normalized face

The Eigen Face method is based on categorizing faces according to the degree of it with a fixed set of 100 to 150 eigen faces. The eigen faces that are created will appear as light and dark areas that are arranged in a specific pattern. This pattern shows how different features of a face are singled out. It has to be evaluated and scored. There will be a pattern to evaluate symmetry, if there is any style of facial hair, where the hairline is, or evaluate the size of the nose or mouth. Other eigen faces have patterns that are less simple to identify, and the image of the eigen face may look very little like a face. Every face is assigned a degree of fit to each of 150 eigen faces, only the 40 template eigen faces with the highest degree of fit are necessary to reconstruct the face with the accuracy of 99 percent. The whole thing is done using Face Recognition softwares [20,9,11,19].

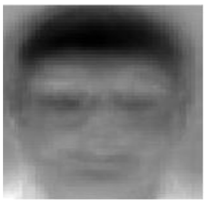


Figure 5: Eigen face

(C) Process Structure:

Facial recognition is a form of computer vision that uses faces to attempt to identify a person or verify its identity. Facial recognition is including following steps to complete the process structure.

Step1: Taking Input image or acquiring the image of an individual’s face either from a digital scan of an existing photograph or acquiring a live picture of a person.

Step2: Locating image or detecting face with the use of some software or tool.

Step3: Analysing face image or extracting its features and focusing on the triangle features such as eyes, nose, lips.

Step4: Comparison or Identification that includes the face print created by the software will be compared to all face prints the system has stored in its database.

Step5: Verification includes match or no match. Software decides whether or not any comparisons from above step are close enough to declare a possible match.

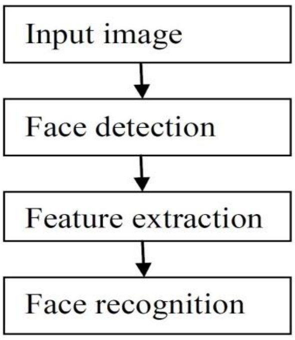


Figure 6: Basic building block of face recognition system

(D) Advantages of using Face Recognition: Following is the list of advantages of using the FRT

[1] One of the top benefits of using bio metric face recognition over other forms of face technology is that this type of biometrics offers a non-contact process. This science makes it easy to capture information from people with biometrics facial technology, since images of the person’s face can easily captured even from a distance.

[2] Instead of requiring a person to offer their fingerprint or asking them to submit iris scaning or retinal scanning. Facial characteristics can be videoed or captured easily without requiring any contact at all. For many purposes, such as crime deterrent or security purposes, the ability to collect biometric facial information without the subject knowing it is extremely important.

[3] Another of the benefits that can be enjoyed with facial recognition biometrics is fast and accurate results. When using biometric face recognition systems, users are able to enjoy high recognition rates and short processing times, making these systems an effective option. Most biometric systems also provide the ability to recognize someones face regardless of facial changes, which may include a different expression, the addition of a beard, or even the addition of glasses. Systems also can accurately recognize your face even if your face is captured from a different vantage point. This advance in biometrics facial technology has made this type of biometrics more user friendly than before.

[4] Reliable face matching is offered by bio metric face recognition systems, which is another advantage of choosing this type of technology. Individual facial features are used by face recognition technology to provide identification and authentication. Biometric face identification software can easily be integrated in to various types of video monitoring systems and various video and graphic formats are supported as well. Most face recognition systems can also be easily adapted to work with existing biometric IT systems that companies are using.

[5] Facial recognition biometric devices offers a range of applications that is highly diverse, including access control, border control, crime fighting, and more. From law enforcement agencies to large corporations with sensitive areas, this biometric technology can provide excellent benefits [13].

(E) Limitations of Facial Recognition Technology

Like any other biometric face recognition also have certain disadvantages. (a) The face can be obstructed by hair, glasses, hats, scarves, etc. (b) also changes in lighting or facial expressions can affect the device as well as technology. (c) a very distinct disadvantage related to face recognition is that people's faces changes over a period of time.

V CONCLUSION

Biometrics is a rapidly developing technology being used widely in various applications such as, forensic, government, social, law enforcement, due to its feature of providing security and authenticity of a particular subject. I this paper we have presented an extensive review of certain important characteristics and various biometric techniques. But certainly it is not possible to definitely state if a biometric technique has a successful run, there are certain factors which can affect the authenticity of a subject like in fingerprint dry/oily finger, in voice recognition cold or illness can affect voice, in face recognition lightening conditions, in iris scan too much movement of head or eye, in hand geometry bandages and in signature scan different signing positions. Among all the biometric techniques Face recognition is the technique which is not intrusive and can be done from a distance even without the user being aware they are being scanned. It can be use purposely for the high security issues like in bank or government offices. Face recognition technology are more reliable, non intrusive, inexpensive and extremely accurate. Currently it is the most challenging recognition technologies which are being widely used.

REFERENCES

[1] Renu Bhatia "Biometrics and Face recognition Techniques", IJARCSSE, vol 3, no. 5, may 2013.

[2] Anil K. Jain "An introduction to Biometric Recognition", IEEE transactions on circuits and systems for video technology, vol 14, no. 1, January 2004.

[3] K P Tripathi, International Journal of Computer Applications (0975 – 8887) Volume 14 No.5, January 2011

[4] http://www.cse.iitk.ac.in/users/biometrics/pages/what_is_biom_more.htm

[5] http://www.hitachi.com/rd/portal/story/idless_biometrics/01.html

[6] EyeDentify, http://www.eyedentify.com/

[7] Zdeneˇk R íhaVáclav Matyáš "Biometric Authentication Systems ", FI MU Report Series, November 2000.

[8] Phil Brimblecombe, "Face detection using neural networks".

[9] A. Ross and R. Govindarajan, "Feature level fusion using hand and face biometrics", In Proc. of SPIE Conf. Biometric Technology for Human Identification II, Mar. 2005, pp. 196-204.

[10] Ion Marques, face recognition algorithms, Proyecto Fin de Carrera, June 16 2010.

[11] S. Z. Li and A. K. Jain, Eds., Handbook of Face Recognition. New York: Springer Verlag, 2004.

[12] J. L. Wayman, "Fundamentals of Biometric authentication technologies" Int. J. Image Graphics, vol 1, no. 1, pp 93-113, 2001.

[13] http://www.biometric-security-devices.com/biometric-face-recognition.html

[14] R. Sanchez-Reillo, C. Sanchez-Avilla, and A. Gonzalez-Macros, "Biometrics Identification Through Hand Geometry Measurements", IEEE Transactions on Pattern Anakysis and Machine Intelligence, Volume 22, Issue 18, Oct. 2000, pp. 1168-
117 1.

[15] D. Zhang and W. Shu, "Two novel characteristic in palmprint verification: Datum point invariance and line feature matching," Pattern Recognit., vol. 32, no. 4, pp. 691–702, 1999.

[16] J. L. Wayman, A. K. Jain, D. Maltoni, and D. Maio, Eds., "Biometric Systems: Technology, Design and Performance Evaluation", New York: Springer Verlag, 2005.

[17] Zhao,W.Y., Chellappa,R.: SFS Based View Synthesis for Robust Face Recognition.
Proceedings of the IEEE International Automatic Face and Gesture Recognition (2000) 285–292

[18] Hu,Y., Jiang, D., Yan, S.,Zhang, L., Zhang, H.: Automatic 3D reconstruction for Face Recognition. Proceedings of the IEEE International Conference on Automatic Face and Gesture Recognition. (2000) 843–850

[19] F. Cardinaux, C. Sanderson, and S. Bengio, "User Authentication via Adapted Statistical Models of Face Images", IEEE Transaction on Signal Processing, Volume 54, Issue 1, Jan. 2006, pp. 361 - 373.

[20] L. Hong and A. K. Jain, "Integrating faces and fingerprints for personal identification", IEEE Trans. Pattern Anal. Mach. Intell., Volume 20, No. 12, Dec. 1998, pp. 1295–1307.

[21] Lee, C.H., Park, S.W.,Chang, W., Park, J.W.: Improving the performance of Multi-Class SVMs in face recognition with nearest neighbour rule. Proceedings of the IEEE International Conference on Tools with Artificial Intelligence. (2003) 411–415