



## A Review on Biometrics and Ear Recognition Techniques

Sukhdeep Singh, Dr. Sunil Kumar Singla(Assit.Prof.)

Electrical & Instrumentation Engg Dept.

Thapar University ,Patiala, India

**Abstract:** *Biometric authentication of a person is highly challenging and complex problem. A significant research effort has gone into this areas and a number of research works were published, Biometrics is a growing technology , which has been widely used in forensics, secured access , prison security, medical, and robotics areas financial services, ecommerce, telecommunication, government, traffic, health care the security issues are more important. Recognizing people by their Ear is relatively new class of biometrics. Several reasons account for this trend: first, ear recognition does not suffer from some problems associated with other non contact biometrics ,such as face recognition; second ,shape and features of ear are unique for each person and invariant with age and structure of the ear is fairly stable and robust to change in facial expressions. It is most promising candidate for combination with the face in the context of multipose face. .In this paper we discuss different methods of Ear detection and recognition*

**Keywords:**

### Introduction

As our society becomes electronically connected to form one big global community through internet and other digital means, it has become necessary to carry out reliable person recognition often remotely and through automatic means. it is most important that who is who ,person who he or she claim's to be because of all financial transaction and of security issues too. It is important to verify that people are allowed to pass some points or use some resources [1]. The security issues are arisen quickly after some crude abuses. For these reason, organizations are interested in taking automated identity authentication systems. Biometrics is automated methods of recognizing a person based on a physiological or behavioural characteristic [18]. Usually there are different methods for verifying identity of individuals: (i) cards, badges, keys are used as identity which very common method (ii) knowledge like password, Personal Identification Number (PIN); (iii) biometrics like fingerprint recognition, face recognition , ear recognition[2]. It is divided into two parts invasive and non-invasive methods. Invasive methods are those that require the cooperation of the subject in order to acquire data needed to compare his biometric features to the ones stored in a database Such as one can allow physical access to a secure area in a building by using finger scans or can grant access to a bank account at an ATM by using retina scan.Noninvasive biometrics does not require the cooperation of the subject [18] ; in fact data capture may be done without their knowledge, Such as scanning a crowd with the help of a camera and using face recognition technology, one can verify matches that are already store in database. These biometric areas have gained the most attention among the research community [17]. There are several application areas where biometrics can be used. Basically there are two types of application scenarios. Identification, "Who I am?" and verification, "Am I who I claim I am?"[1]. In identification there is a database with biometrics and the just taken biometric, e.g. hand shape is compared with the biometrics in database and system decides who the person is? In verification the comparison is done only with data, which is known to be valid for the approved person, e.g. the fingerprint or hand shape is included in an identification card[1]

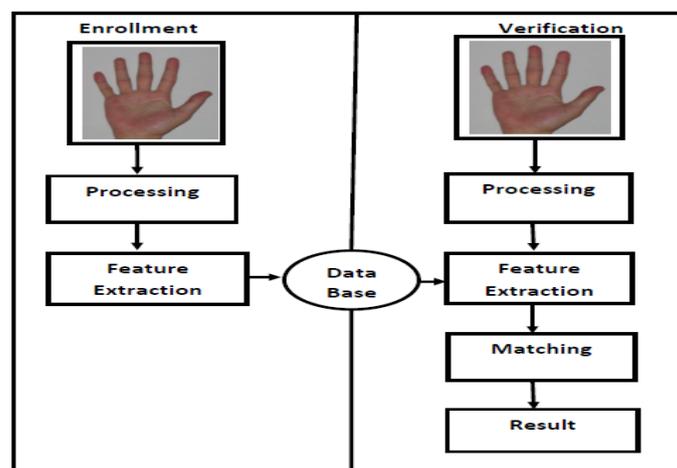


Fig1: General Biometric System[3].

In Fig 1 shows typical architecture of all biometric systems consists of two phases[3]:

- Enrollment,
- Authentication.

Enrollment: several images of hand are taken from the users. The images, called templates, are pre-processed to taken to feature extraction part , where a set of measurement is performed by using some tools by using automated systems in different software like matlab and LabVIEW.it depends on the method used for recognition. Models for each of the users is then stored in the database. Authentication: a single picture is taken, pre-processed, and features are obtained. In the proposed system, the process of verification is used, where the input template is compared only with the model of claimed person. The feature vector is compared with features from the model previously stored in the database. The result is the person is either authorized or not authorized

The most commonly used biometrics are fingerprints, face, voice, iris, signature, and hand geometry, ear biometrics shows in Fig 2.

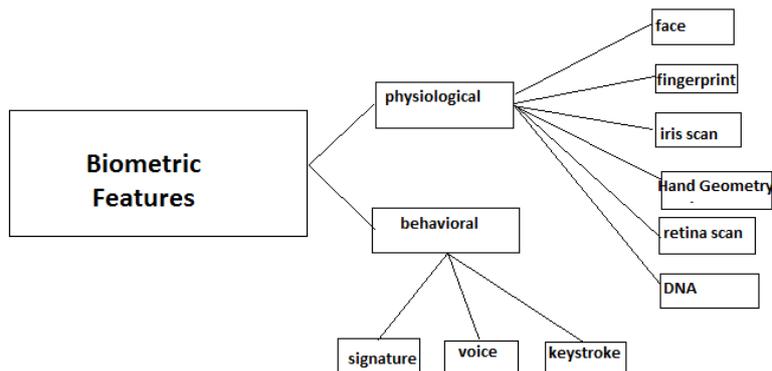


Fig 2: Biometrics systems [4].

Biometrics can measure both physiological and behavioural characteristics [4].

**Physiological biometrics**-based on measurements and data derived from direct measurement of a part of the human body.

**Behavioural biometrics**-based on measurements and data derived from an action.

Physiological biometrics are:

- a. Finger-scan
- b. Facial Recognition
- c. Iris-scan
- d. Retina-scan
- e. Hand-scan

Behavioural biometrics are:

- a. Voice-scan
- b. Signature-scan
- c. Keystroke-scan

Some of the important biometric system are:

#### **Fingerprint recognition**

It is the most widely used biometric technology. Fingerprint uniqueness can be defined by analyzing the trivia of a human being. Trivia is include sweat pores, distance stuck between ridges and bifurcation [5].

#### **Advantages of finger print recognition**

- Subjects have multiple fingers
- Easy to use.
- systems require less space

#### **Disadvantages of finger print recognition**

- Public Perceptions
- Privacy concerns of criminal implications

#### **Facial recognition**

Facial recognition is an automatic method to record the geometry of distinguish features of the face. Different methods of facial recognition among various vendors all focus on measures of key features [6].

#### **Advantages of facial recognition**

- No contact required for recognition.
- Commonly available cameras used

#### **Disadvantages of facial recognition.**

- Face can be obstructed by hair, glasses, hats, etc. sensitive to changes in lighting, expression, and pose.
- Faces change with time.

#### **Signature recognition**

It is the process used to recognize an individual's signature. Dynamic signature verification technology uses the behavioural biometrics of a hand written signature to confirm the identity of a computer client[7].

#### **Advantages of signature recognition:**

- Possible detection of inconsistent user during enrollment stage;
- Fast and simple training;
- Cheap hardware.
- Little storage requirements;

#### **Disadvantages of signature recognition:**

- Signature verification is designed to verify subjects based on the traits of their 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.
- Error rate: 1 in 50.

#### **Palm recognition**

In palm recognition a 3-dimensional image of the hand is collected and the feature vectors are extracted and compared with the database feature vectors[8]. The evolution of the human blueprint has allowed them both to share virtually all of the same detectable characteristics as fingerprints. The major difference is that the palm is larger and can therefore yield a greater number of minutiae points to be used for comparison of the sample biometric to the stored biometric template

#### **Advantages of Palmprint Biometrics:**

- Since the palm area is much larger, hence more distinctive features can be captured compared to fingerprints. This makes it more even more suitable in identification systems than fingerprints.

#### **Disadvantages of Palmprint Biometrics:**

- The palmprint scanners are usually bulkier and expensive since they need to capture a larger area than the fingerprints scanners.

#### **Hand geometry**

Hand or finger geometry is an automated measurement of many dimensions of the hand and fingers. It has 3-D image of top and sides of hand and fingers is collected and the feature vectors are extracted and compared with the dataset feature vectors[9]. It has 3-D image of top and sides of hand and fingers is collected and the feature vectors are extracted and compared with the dataset feature vectors. It is recognition devices are bulky but identification is done in a seconds. User places hand, palm-down, on a metal surface with guidance pegs. Pegs are used to confirm that fingers are positioned correctly and also verify correct hand position

#### **Advantages hand geometry.**

- Acquisition convenience and good verification performance of system,
- Suitable for medium and low security application.
- Works in harsh environments.

#### **Disadvantages of hand geometry.**

- Large size of hand geometry device is needed.
- Single hand use only in one time.
- Not highly unique.

#### **Voice recognition**

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 [10]. The person to be identified is usually required to speak a secret code, which facilitate the verification process

#### **Advantages of voice recognition.**

- Public acceptance
- No contact required

#### **Disadvantages of voice recognition.**

- Difficult to control sensor and channel variances that significantly impact

Capabilities.

- Not sufficiently distinctive for identification over large databases

#### Iris Scan

The iris scans process for this a specialized camera is required, naturally very close to the subject, uses an infrared imager to illuminate the eye and capture a very high-resolution image [11, 17]. Complete process takes only few seconds and provides the details of the iris knowingly produce, recorded and stored in dataset for future identification and verification

#### Advantages of iris scan

- No contact required
- Protected internal organ; less prone to injury
- Believed to be highly stable over lifetime

#### Disadvantages of iris scan.

- Difficult to capture for some individuals
- Easily obscured by eyelashes, eyelids, lens and reflections from the cornea

#### Retina Scan

Retina Scan is a biometric technique that uses the unique patterns on a person's retina to identify them It is based on the blood vessel pattern in the retina of the eye[12]. Retina scan technology is older than the iris scan technology that also uses a part of the eye. The first retinal scanning systems were launched by Eye Identify in 1985

#### Advantages of retina scan:

- Very high accuracy.
- There is no known way to replicate a retina.

#### Disadvantages of retina scan:

- Very intrusive.
- It has the stigma of consumer's thinking it is potentially harmful to the eye.
- Very expensive.

#### DNA

Each person's DNA is unique except for identical twins .It can thus be considered a 'perfect' modality for identity verification. , DNA techniques are currently being used by Law enforcement [13].

#### Advantages of DNA

- very accurate method

#### Disadvantages of DNA.

- it is expensive method
- it take so much time about 4 to 5 hours

#### Comparison of Various Biometric Technologies:

The choice of a particular human characteristic to be used as a biometric trait depends on the following criteria [14]:

- **Uniqueness** is how well the biometric separates individually from another.
- **Permanence** measures how well a biometric resists aging.
- **Collectability** ease of acquisition for measurement.
- **Performance** accuracy, speed, and robustness of technology used.
- **Acceptability** degree of approval of a technology.
- **Universality** the quality of being universal; existing everywhere.

BIOMETRICS	UNIVERSALITY	UNIQUENESS	PERMANENCE	COLLECTABILITY	PERFORMANCE	ACCEPTABILITY
Face	H	L	M	H	L	H
Fingerprint	M	H	H	M	H	M
Hand Geometry	M	M	M	H	M	M
Ear	H	H	M	M	M	H
Iris	H	H	H	M	H	L
Retinal scan	H	H	M	L	H	L
Signature	L	L	L	H	L	H
Voice	M	L	L	M	L	H
DNA	H	H	H	L	H	L

Fig 3: comparison of various biometric techniques with its strengths and weakness[14].

### Ear Recognition Ear topology

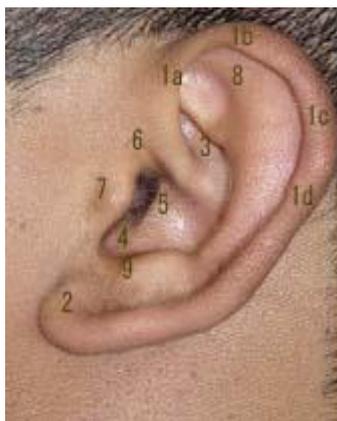


Fig 4: ear topology [1].

in Fig 4 shows the part of ear which are following:

- 1) Helix Rim
- 2) Lobule
- 3) Antihelix
- 4) Concha
- 5) Tragus
- 6) Antitragus
- 7) Crus of Helix
- 8) Triangular Fossa
- 9) Incisure Intertragica

#### Why Ear Recognition over other Technology?

There are number reasons to choose ear recognition is following:

- a) Ear biometrics are convenient and because their acquisition tends to be perceived as less invasive.
- b) It is accurate and allows for high enrolment and verification rates.
- c) It does not require an expert to interpret the comparison result.
- d) It can use with existing cameras and image capture devices will work with no problems.

Ear detection has collect little attention match up to other popular biometrics such as face, fingerprint and gait. Ear is a workable new class of biometrics since the ear has desirable properties such as universality, distinctiveness and stability. Previous research has suggested the use of ears as a biometric for human identification. Researchers have advocated that the shape and appearance of the outer ear for humans is unique, and relatively unchanged throughout the lifetime of an individual. Although no one has proved that each person's ears are unique, studies in [1, 2]. gave empirical supporting evidence, Face changes radically based on expression, that problem does not exist with ears

In addition, the immediate background of the ear is very predictable it is always located on the side of the head, whereas facial recognition typically requires a controlled background for accurate capture a situation that is obviously not always present. Unlike iris, retina, or fingerprint capture which are contact biometrics, the ear does not require close proximity to achieve capture. Figure shows the common terminology of the external ear. Ears have played a significant role in forensic science.

All identification or authentication technologies operate using the following four stages[1,2]:

- a) **Capture:** A sample is captured by the camera during Enrolment and also in identification or verification process, it is taken by any digital camera and easy to use .
- b) **Extraction:** by this unique data is extracted from the sample by using different techniques and a template is created by using it on different platforms like matlab and Lab VIEW.
- c) **Comparison:** the template is then compared with a sample .
- d) **Match/non match:** ear recognition is very complex technology and is largely software based, the system decides if the features extracted from the new samples are a match or a non match.

All steps of ear recognition are shown in Fig 5.

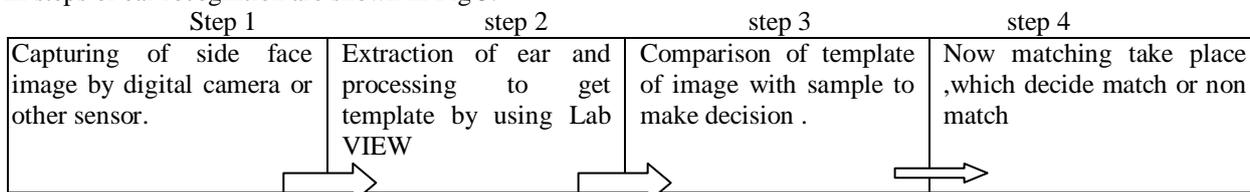


Fig 5: steps of ear recognition [1,2,4]

Ear biometrics is a relatively unexplored biometric field, but has received a growing amount of attention over the past few years. There are three modes of ear biometrics: ear photographs, ear prints obtained by pressing the ear against a flat plane, and thermograph pictures of the ear. The most common implementation of ear biometrics is via photographs for automated identification applications, the most common implementation of ear biometrics is via photographs for automated identification applications. In practice, and we discuss some worked done on ear recognition. One of the first ear recognition systems is the Iannarelli's system which was originally developed in 1949. This is a manual system based upon 12 measurements. Each photograph of the ear is aligned such that the lower tip of a standardized vertical guide on the development easel touches the upper flesh line of the cocha area, while the upper tip touches the outline of the ant tragus. Then the crus of helix is detected and used as a centre point. Vertical, horizontal, diagonal, and anti-diagonal lines are drawn from that centre point to intersect the internal and external curves on the surface of the pinna. The 12 measurements are derived from these intersections and used to represent the ear[15]. Mark Burge and Wilhelm Burger reported the first attempt to automate the ear recognition process in 1997, they used a mathematical graph model to represent and match the curves and edges in a 2D ear image. Some years later, Belén Moreno, Ángel Sanchez, and José Vélez described a fully automated ear recognition system based on various features such as ear shape and wrinkles. Since then, researchers have proposed numerous feature extraction and matching schemes, based on computer vision and image processing algorithms, for ear recognition [2]. Chen and Bhanu developed another shape model-based technique for locating human ears in side face range images where presented a 3D ear recognition system that exploited the depth and structure of the ear's morphological components They started by locating the edge segments and grouping them into different clusters that are potential ear candidates. For each cluster, they register the ear shape model with the edges[16].

The use of 2D or 3D ear images for human recognition differs from the use of *ear prints*: marks left by secretions from the outer ear when someone presses up against a wall, or some platform . Ear prints have been introduced as physical evidence in several criminal cases in the many countries, although some convictions that relied on ear prints have been overturned. Ear prints haven't been widely accepted in court due to a lack of scientific consensus as to their individuality. In addition, the use of ear thermo grams could help mitigate the problem of occlusion due to hair and accessories. As the technology matures, both forensic and biometric domains will benefit from this biometric

## Conclusions

Different approaches for ear recognition were discussed in this paper biometrics play a important role in personal identification, the importance of biometrics in every day life has been discussed and different biometrics technologies are introduced. it has been shown that ear biometrics can be used for identification and for the further development it is a good biometric and is comparable to that of face .

## References

- [1] A.K. Jain, Next Generation Biometrics, Department of Computer Science & Engineering, Michigan State University.
- [2] Mark Burge and Wilhelm Burger. "Ear Biometrics". BIOMETRICS: Personal Identification in a Networked Society, p.273-286.1999.
- [3] ] A.K jain.; Bolle, R.; Pankanti, S., eds. *Biometrics: Personal Identification in Networked Society*. Kluwer Academic Publications. ISBN 978-0-7923-8345-1,1999
- [4] "[CHARACTERISTICS OF BIOMETRIC SYSTEMS](#)". Cernet.
- [5] Necla Ozkaya, Seref Sagiroglu, Arif Wani, "An Intelligent Automatic Fingerprint Recognition System Design," icmla, pp.231-238, Fifth International Conference on Machine Learning and Applications (ICMLA'06), 2006
- [6] R. Brunelli and T. Poggio, "Face Recognition: Features versus Templates", IEEE Trans. on PAMI, (15)10:1042-1052,1993.
- [7] J.Chapran. "Biometric Writer Identification: Feature Analysis and Classification". *International Journal of Pattern Recognition & Artificial Intelligence* 20: 483–503,2006.
- [8] D. Zhang . "Palmpoint Authentication", Kluwer Academic Publishers,2004.
- [9] Nongluk Covavisaruch, Pipat Prateepamornkul "Personal Verification and Identification Using Hand Geometry" ecti transactions on computer and information technology vol 1 ,Nov 2005.
- [10] S.Anderson, N. Liberman, E.Bernstein,S. Foster.,E. Cate, & B.Levin Recognition of elderly speech and voice-driven document retrieval. *IEEE International Conference on Acoustics, Speech, and Signal Processing. Proceedings. ICASSP99, 15-19 March 1999*, Phoenix, AZ, USA. IEEE; Signal Process. Soc, 145-8 vol.1,1999.
- [11] M.S.Hosseini.; B.N.Araabi, H.Soltanian-Zadeh, "Pigment Melanin: Pattern for Iris Recognition". *IEEE Trans Instrum Meas* 59 (4): 792– 804.doi:10.1109/TIM.2009.2037996,2010.
- [12] Iris/Retinal Identification. Wcu.Edu. Retrieved on 2007.
- [13] Colin Pitchfork — first murder conviction on DNA evidence also clears the prime suspect Forensic Science Service Accessed 23 December 2006
- [14] Comparisons of Various Biometric Technologies, www.biometricvision.com
- [15] A. IANNARELLI. Ear Identification, Forensic Identification Series. Paramount Publishing Company, Fremont, California,1989
- [16] H. CHEN AND B.BHANU. Human ear detection from side face range images. In Proc. of the International Conference on Pattern Recognition ICPR. Cambridge, UK, 574-577,2004.

- [17] SUNIL KUMAR SINGLA, AND PARUL SETHI.Challenges at different stages of an iris based biometric system. Songklanakarin J. Sci. Technol. 34 (2) 189-194, Mar. - Apr. 2012.
- [18] SUNIL KUMAR SINGLA AND AJAT SHATRU ARORA ,speaker verification system using LabVIEW.IETE technical review ,Vol 24,No 5,pp 403-412 ,september -october 2007.