IJITKM 0973-4414 Volume-9, Number-2 Jan-Jun 2016 pp. 14-20 **Impact Factor 2.8** available online at www.csjournalss.com

# Biometric Technology: An Evolution

[1]Karan Singh, [2]Nippun Kamboj
[1] Research Scholar, Department of Comp. Sci. & App. K.U. Kurukshetra, Haryana, India
[2] Research Scholar, Department of Comp. Sci., MM University, Mullana, Haryana, India
karanola123@gmail.com, nippunkamboj@gmail.com

**Abstract:** Founding identity of any user (person) in widely organized social or business environment is a critical task. Whenever a user wants to access any type of facility of secure environment a question arise for this type of situation as, "Is this authorized person or not to use this facility?" Checking and verifying is used to granting access to any user or inhibit any unauthorized user. For granting access into system (finding authorized/unauthorized) many techniques are used, Biometrics is one of them. Biometrics, defined as the disciplineof identifying a user based on his/herbiologically or behavioralfeature. A biometric system is basically a pattern recognition system that identifies a person (user) by defining his/ her different biological characteristics.Biometrics biologicalfeatures are genetically implied like a person's iris, retina, finger, face, vascular structure etc. Social/Behavioral characteristics are that any one learns like a handwritten signature, a person's gait, typing dynamics or voice characteristics etc. Biometrics systemsare used in business, social and forensic applications for establishing identity. In this paper various biometricstechniques and their comparative characteristics are disused.

**Keywords:** Biometrics, Biometric system types, Biometrics technology.

## I. INTRODUCTION

Biometrics systems are recognition system based on person's biological and behavioral features. In these days biometrics features are face recognition, iris scan, retina-scan, finger prints, voice and handwriting etc. In current trends, biometrics is key to identify any individuals to access business and forensic application. Biometric system is now getting growth and becoming the basis of a highly secure identification and personal verification. In biometrics identification process at user level basic biological "data collection" is made i.e. finger print characteristics, retina-scan, voice etc. These characteristics are sampled and then extracted by "signal processing" for pattern matching with templates in biometrics database storage. After that "decision" is given to accept or reject that user which leads to an authorized/unauthorized user (see in figure 1).

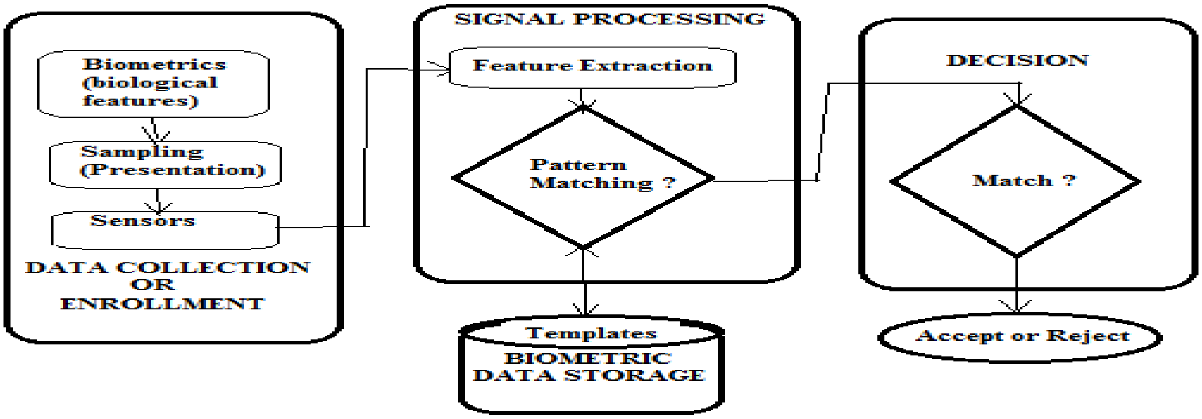


Figure 1: General Biometric System

Any developed biometric system thus may have some common steps (see in figure 2) which involved in identifying any individuals according to their biological features. These are Sampling, Preprocessing, Feature extraction, Quality control and Recognition [1].

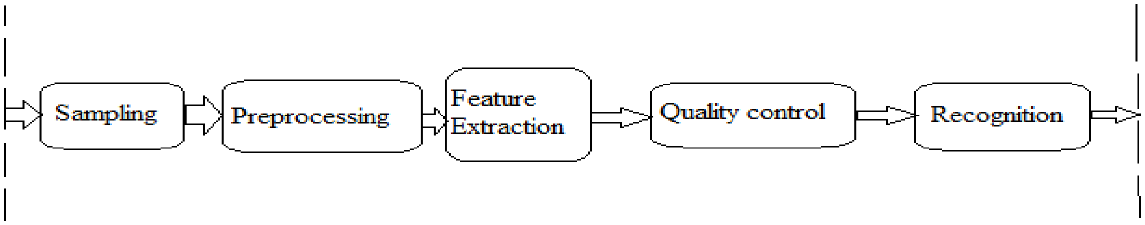


Figure 2: Common Steps Involved In Developing Any Biometric System

## II. BIOMETRICS SYSTEM TYPES

There are two types of biometrics system [2] to identifying any person in a given pool of data templates. These are Verification/Authentication(One-to-One method) [3] andIdentification (One-to-Many method) [3].

**2.1 Verification/Authentication(One-to-One method)**:In this case, user's templates may already store in a central biometrics database for claim [2].In a verification method, an already registereduser claims an identity and the system verifies the authenticity of the claim based on his/her collected biometric feature. Example: accessing bank account after retina-scanning.

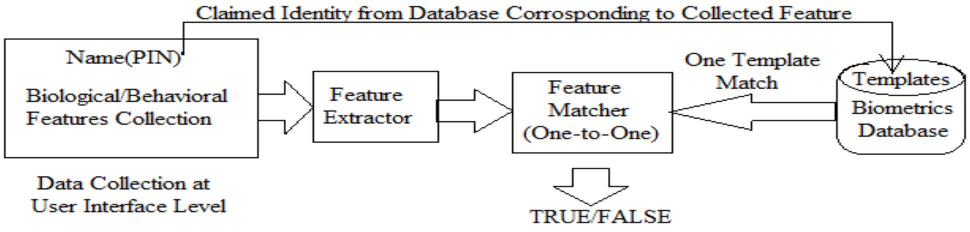

Claimed Identity from Database Corrosponding to Collected Feature
Name(PIN)
Biological/Behavioral Features Collection
Data Collection at User Interface Level
Feature Extractor
Feature Matcher (One-to-One)
One Template Match
Templates
Biometrics Database
TRUE/FALSE

Figure 3: Verification/Authentication (One-to-One method)

**2.2 Identification (One-to-Manymethod):** Biometrics can be used to define a person's identity even without his cognizance[2]. Identification based biometric system identifies aregistered user based on his/her biometric features without the user having to claim an identity. Scanningcrowd with the help of a camera and using face recognition technology, one can verify matches that are already store in biometrics database (see in figure 4).

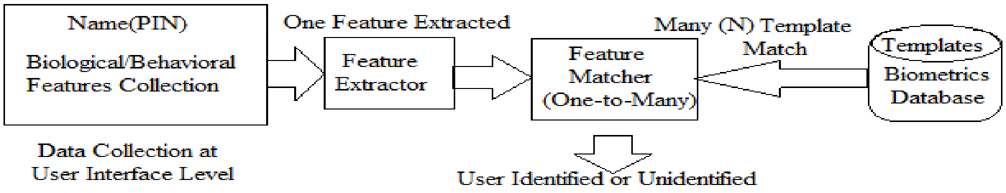

Name(PIN)
Biological/Behavioral Features Collection
Data Collection at User Interface Level
One Feature Extracted
Feature Extractor
Feature Matcher (One-to-Many)
Many (N) Template Match
Templates
Biometrics Database
User Identified or Unidentified

Figure 4: Identification (One-to-Many Method)

DOI: 10.141079/IJITKM.2016.912

In biometrics, biometric system can be categorized into two modules, as follows:-
(I) Database Planning Module.
(II) Verification/Identification Module.
Database Planning Module can next be divided into two sub-modules:-
(i) Enrollment Module (ii) Training Module while the other module
Verification modulecan also divided into two parts as:-
(i) Matching Module and (ii) Decision Module.

## III. BIOMETRICS TECHNOLOGIES

Many biometrics technologies (see in figure 5) are used in these days. Widely used biometrics technologies are these:-

- Fingerprint recognition
- Face recognition
- Iris-scan
- Retina-scan
- Signature recognition
- Hand geometry
- Signature scan
- Keystroke scan
- Palm scan
- Voice recognition

**Primary biometric disciplines include:**Fingerprint, Facial recognition (optical and thermal) Voice recognition, Signature-scan, Iris-scan, Retina-scan, Hand geometry, Keystrokescan, Palm-scan are basic primary biometric disciplines.

**Fact-finding/Exploratory stages include:**DNA, Ear shape, Odor, Finger geometry (shape and structure of fingers), Gait recognition (style of walking), Vein-scan (in back of hand or beneath palm) are exploratory disciplines.

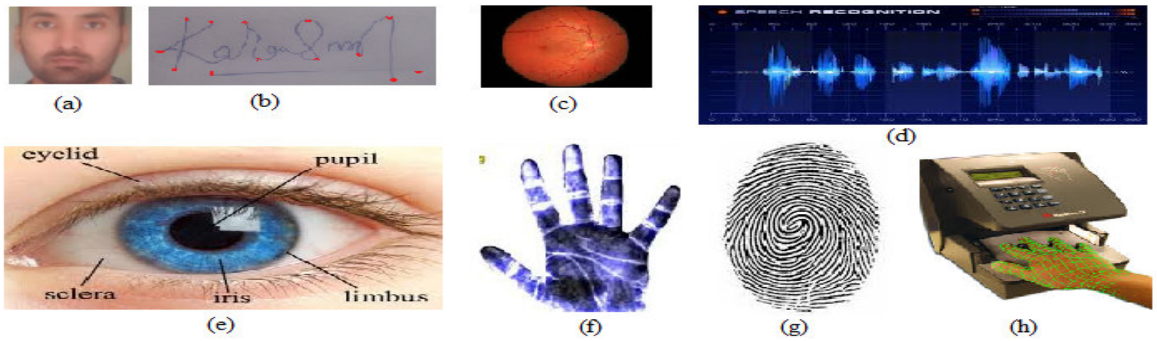


Figure 5: Biometric Traits: (a)Face, (b)Signature, (c)Retina, (d)Voice, (e)Iris, (f)Palm scan, (g)Fingerprint, (h)Hand Geometry.

**3.1Face Recognition:** Facedifferentiatesone person to another as biometric traits. Face recognition records the three-dimensional geometry of unique features of the face. Face recognition technique is used for identifying any persons, criminals, and other types of persons for law administration purposes. It requires camera as equipment for user identification. Facial recognition is a form of computer vision that uses faces to attempt to identify a person or verify a person's claimed identity. Facial recognition biometric process is including five steps (See in figure 6) to complete their process [5].

Step1:Obtaining theimageofuserface.
Step2:Locateimageofface.
Step3:Analysisoffacialimage.
Step4:Comparisonofcapturedfaceagainststoredtemplates.
Step5:Matchornomatch.

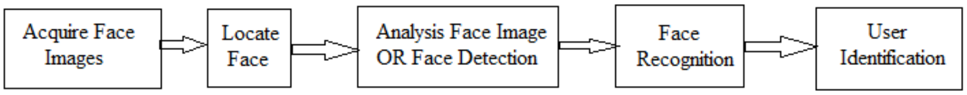


Figure 6: Steps in Face Recognition Biometric System

**3.2Signature Recognition:**Signature recognition biometric system is used to identify anyusers hand-written or signature [6]. Dynamic signature verification technology uses the behavioral biometrics of a hand written signature to check the identity of a computer client. Examining the figure, speed, stroke, and pen stress and timing information during the act of signing natural way.

**3.3Retina Scan:**Retina scan biometric system is based on the blood vessel pattern in the retina of the eye [7]. 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 vessel 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.

**3.4 Voice Recognition:**Voice recognition biometric technology does not acquire the visual structures of the human body this captured behavioral feature. Sound sensations of a person is measured and matched to an existing biometric template dataset. The person to be identified is usually required to speak a secret code, which lead the verification process.

**3.5 Iris Scan:**The iris is the colored ring of textured tissue that surrounds the pupil of the eye. Even twins have different iris patterns and everyone's left and right iris is different, too. This unique biological feature leads to a new biometric identification system known as iris-scan[8]. The probability that 2 different irises could produce the same iris code is estimated as low as 1: 1078 the probability of two persons with the same iris is very low (1: 1052) [9].

**3.6 Palm Recognition:** In palm recognition biometric system a 3-D image of the hand geometry is captured and the unique features are extracted and matched with the database templates for identify user [10]. (Palm recognition process is shown in figure 7.)

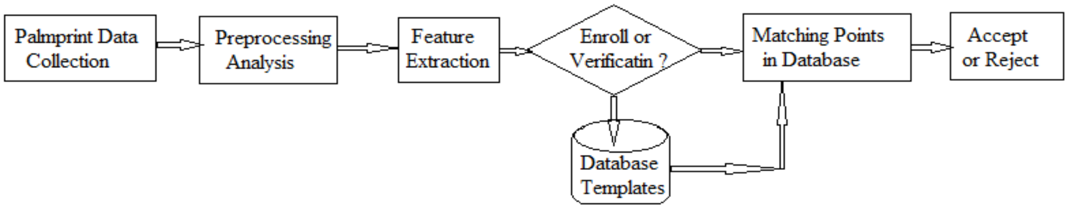


Figure 7: Process of Palm recognition Algorithm.

**3.7 Finger Print:**Fingerprints are used for unique personal biometric biological identification [11].Fingerprints of identical twins are different and so are the prints on each finger of the same person thus suitable for biometric identification. The accuracy of the currently available fingerprint recognition systems is suitable for authentication systems involving a few hundred users. It is probable that the likelihood of two individuals having the same fingerprint is less than one in billion.

**3.8 Hand Geometry:**Hand geometry has 3-D image of top and sides of hand and biological features of hand and fingers like hand shape, length and widths of figure, size of palm and wrinkles in palm are captured for uniquely define a person. These features are collected and compared with the dataset templates of biometric template [12]. Basic steps include in biometric algorithms of hand geometry are as follows:-

Step 1: Hand image acquisition.

Step 2: Image Preprocessing/Analysis and capture/calculate finger & palm features.
2.1: Finger Baselines
2.2: Finger Lengths
2.3: Finger Widths
2.4: Palm Width etc.

Step 3: Feature Extraction.

Step 4: Match calculated feature with pre-stored biometrics database templates.

Step 5: result as authorized/unauthorized user.

## IV. COMPARISIONS OF BIOMETRIC TRAITS BASED ON BIOMETRIC CHARACTERSTICS

Biometric systems having many qualities according to their use, which are measured as High (H), Medium (M) and Low (L). Here some biometric traits are disused [13][14] (See in table 1).

**Universality:** Every person should have the unique biometric characteristic.

**Permanence:** The biometric characteristic should be invariant over time.

**Uniqueness:** No two persons should be the same in terms of the biometric characteristic.

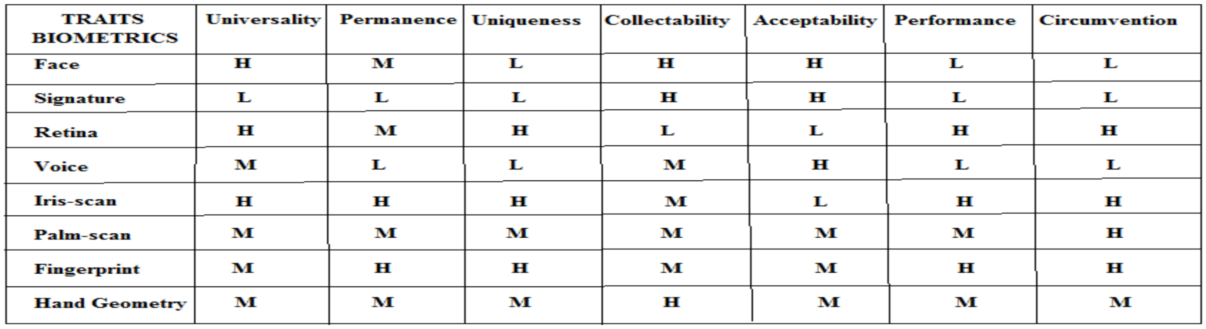
**Collectability**: The biological/behavioral biometric features should be computable with some sensing device.

**Acceptability:** The particular user and the public generally should not have any objections to the collection of the biometric feature.

**Performance:** Refers to the level of accuracy and speed of recognition of the system given the operational and environmental factors involved.

**Resistance to Circumvention:** Refers to the degree of difficulty required to defeat or bypass the system.

Table 1 : Comparision of Various Biometrics Traits/Features.



| TRAITS BIOMETRICS | Universality | Permanence | Uniqueness | Collectability | Acceptability | Performance | Circumvention |
|---|---|---|---|---|---|---|---|
| Face | H | M | L | H | H | L | L |
| Signature | L | L | L | H | H | L | L |
| Retina | H | M | H | L | L | H | H |
| Voice | M | L | L | M | H | L | L |
| Iris-scan | H | H | H | M | L | H | H |
| Palm-scan | M | M | M | M | M | M | H |
| Fingerprint | M | H | H | M | M | H | H |
| Hand Geometry | M | M | M | H | M | M | M |

DOI: 10.141079/IJITKM.2016.912

## V. ADVANTAGES AND DISADVANTAGES OF BIOMETRIC TECHNOLOGY

As these technologies are growing fast but some strength and weakness also occurred with each biometric technology [15].

**Facial recognition:**

Advantages: Non-intrusive, Cheap technology.
Disadvantages: 2D recognition is affected by changes in lighting, the person's hair, the age, and if the person wear glasses.Require camera equipment for user identification.

**Signature-scan:**

Advantages: Non-intrusive, Little time of verification (about five seconds), cheaptechnology.Disadvantages: 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.

**Retinal scanning:**

Advantages: Very high accuracy, There is no known way to replicate a retina.
Disadvantages: Some disadvantages related to retina scan are as follows:-
i) Very intrusive.
ii) It has the stigma of consumer's thinking it is potentially harmful to the eye.
iii) Comparisons of template records can take upwards of 10 seconds, depending on the size of the database.
iv)Very expensive.

**Voice Recognition:**

Advantages: Non-intrusive, high social capability, less verification time is about five seconds and not expensive technology.
Disadvantages: A person's voice can be easily recorded and used for unauthorized PC or network, Low accuracy, an illness such as a cold can change the voice of a person, which makes identification difficult or impossible.

**Iris Scan:**

Advantages: Very high accuracy, Verification time is generally less than 5 seconds.Disadvantages: Disturbing, Very expensive.

**Palm Scan:**

Advantages: 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: The palm print scanners are usually bulkier and expensive since they need to capture a larger area than the fingerprints scanners.

**Fingerprint Scan:**

Advantages: Very high accuracy, economically affordable for everyone, it is one of the most developed biometrics, Easy to use, small storage space required for the biometric template.
Disadvantages:For some people it is very intrusive, because is still related to criminal identification, it can make mistakes with the dryness or dirty of the finger's skin, as well as with the age.

**Hand Geometry:**

Advantages: It can be easily integrated into other devices or systems.
Disadvantages: Very expensive, large size of hardware system.

## VI. CONCLUSION

Biometrics technology is a fastdeveloping technology that is being broadly used in forensics, security, law enforcement; prevent unauthorized access in ATMs and work places and in computer networks. There are many forms of biometrics now being built into technology platforms. There are lots of applications and solutions in biometrics technology used in security systems. But it is not possible to definitely state if a biometric technique are successful run, it is essential to locate factors that's help to reduce affect system performance. The international biometric group Strike System Strikes are:in Facial recognition Lighting conditions, in Fingerprint Dry/oily finger, in Voice recognition Cold or illness that affects voice, in Iris-scan Too much movement of head or eye, in Hand geometry Bandages, and in Signature scan Different signing positions. Face recognition technology are more reliable, non-intrusive, inexpensive and extremely accurate. Currently Face recognition and fingerprint technologies are the most challenging recognition technologies.

## REFERENCES

[1]Markus, Miroslav and Mirko, Towards a General Definition of Biometric Systems, IJCSI International Journal of Computer Science Issues, Vol. 2, 2009, ISSN (Online): 1694-0784, ISSN (Printed): 1694-0814

[2] Biometric Recognition: Security and Privacy Concerns, Salil Prabhakar, Sarath pankanti, Anil K. Jain: publishedbythe IEEE computersociety.

[3] http://abibiometrics.org/comparison-of-the-1-1-and-1-n-authentication-methods.html

[4] Renu Bhatia et al., International Journal of Advanced Research in Computer Science and Software Engineering 3(5),May - 2013, pp. 93-99.

[5] Bonsor, K. "How Facial Recognition Systems Work" Retrieved 2008-06-02.

[6] Smita S. Mudholkar, Pradnya M. Shende, and Milind V. Sarode: Biometric Authentication Techniquefor IntrusionDetectionSystemsusing FingerprintRecognition: International Journal of Computer Science, Engineering and Information Technology (IJCSEIT), Vol.2, No.1, February 2012.

[7]Sugandha Agarwal1, Rashmi Dubey2, Sugandha Srivastava3, Prateek Aggarwal: A Comparative Study of Facial, Retinal, Iris and ScleraRecognition Techniques: IOSR Journal of Computer Engineering (IOSR-JCE)e-ISSN: 2278-0661, p- ISSN: 2278-8727Volume 16, Issue 1, Ver. VI (Feb. 2014), PP 47-52.

[8]Vanaja Roselin.E.Chirchi Dr.L.M.Waghmare, E.R.Chirchi: Iris Biometric Recognition for Person Identification inSecurity Systems: International Journal of Computer Applications (0975 – 8887)Volume 24– No.9, June 2011.

[9] Harbi AlMahafzah, Ma'en Zaid AlRwashdeh: A Survey of Multibiometric Systems.

[10] Sumalatha K.A, Harsha H: Biometric Palmprint Recognition System: A Review: International Journal of Advanced Research in Computer Science and Software Engineering 4(1),January - 2014, pp. 429-433.

[11]Finger print: Le Hoang Thai 1 and Ha Nhat Tam: Fingerprint recognition using standardized fingerprint model: IJCSI International Journal of Computer Science Issues, Vol. 7, Issue 3, No 7, May 2010 ISSN (Online): 1694-0784 ISSN (Print): 1694-0814.

[12]R. Sanchez-Reillo, C. Sanchez-Avila, and A. Gonzales-Marcos, "Biometric identification through hand geometry measurements," IEEETrans. Pattern Anal. Mach. Intell., vol. 22, no. 10, pp. 1168–1171, Oct. 2000.

[13] Iridian Technologies, http://www.iriscan.com.

[14] D. Maltoni, D. Maio, A. K. Jain, and S. Prabhakar, Handbook of Fingerprint Recognition. New York: Springer Verlag, Jun. 2003.

[15]Ad: http://biometrics.pbworks.com/: Advantages and disadvantages of technologies.