AN OVERVIEW OF BIOMETRICS

JAMMI ASHOK [1]
Professor and Head
Department of IT,
GCET, Hyderabad, India.

VAKA SHIVASHANKAR [2]
Assistant Professor
Department of MCA
KCCS, Warangal

P.V.G.S.MUDIRAJ [3]
Associate Professor,MCA Dept.
Adams Engg. College,
Paloncha,Khammam.

Abstract

The term biometrics is derived from the Greek words bio meaning "life" and metrics meaning " to measure" . Biometrics refers to the identification or verification of a person based on his/her physiological and/or behavioral characteristics. Several verification/identification based biometrics have evolved based on various unique aspects of human body, ease of acquiring the biometric, public acceptance and the degree of security required. This paper presents an overview of various biometrics in use/proposed and their applicability to different activities.

Keywords: Biometrics, FMR, FNMR, ROC, CMC

1. INTRODUCTION

1.1 NEED FOR BIOMETRICS

In the present times, when most transactions - financial or otherwise - are automated and many of them networked, security has emerged as a most important issue . Security is usually in the form of possessions (like ID cards , keys) or secret knowledge (like password , PIN) . This type of security is not failsafe as for example, ID cards may be lost ; passwords may be forgotten or compromised [1] . A strong need was thus felt for more robust authentication methods and extensive research ensued in this area. This led to the concept of using human body parts or human mannerism itself as security and authentication measure, and finally to the emergence of biometrics as a field by itself . It is now widely accepted that any positive identification of a person must include biometric identification [1] .

1.2. PREREQUISITES OF A GOOD BIOMETRIC

Any aspect of human physiology or behavior that can be accepted as a biometric should satisfy five properties described by Clarke which are as follows :

a) Universality : Every person should have the biometric characteristic.

b) Uniqueness : No two persons should be the same in terms of the biometric characteristic

c)Permanence: The biometric characteristic should be invariant over time.

d)Collectability: The biometric characteristic should be measurable with some practical sensing device.

e)Acceptability: The public should have no strong objection to the measuring or collection of the biometric.

2. TYPES OF BIOMETRICS

Based on the above guidelines, several biometrics are being developed and are in use .This paper describes popularly used biometrics in terms of the character measured , the devices used to collect the biometric , features extracted , the algorithms used and the areas of applicability.

2.1 FINGERPRINT BIOMETRIC METHOD

Fingerprint identification is popular because of their ease in acquisition, number of sources (ten fingers) and their acceptance over a long time by law enforcement offices. Fingerprints form part of an individual's phenotype and are not determined by genetics and hence qualify as good biometric. A fingerprint appears as a series of ridges with pores (sweat glands) and valleys between these ridges as shown in fig1. In a fingerprint a minutia is a point where a ridge ends or splits. A typical finger would have 30 to 60 minutia points. Minutia is the feature which is extracted for fingerprint biometric .

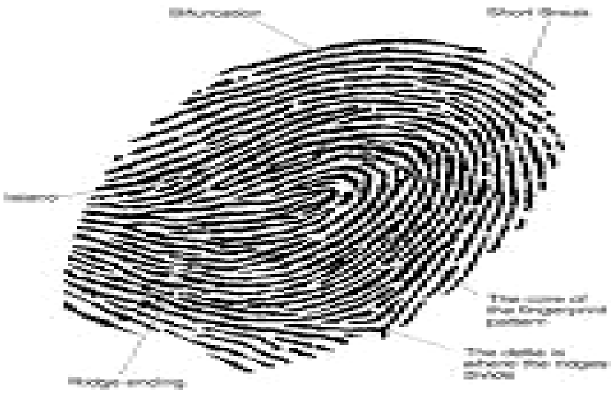

Bifurcation
Short Break
Island
The core of the fingerprint pattern
The delta is where the ridges divide
Ridge ending

Fig1: A typical minutia map

Four technologies are in use to extract fingerprint images. These are as listed below

a)Optical Sensors : These sensors capture *visual image* of finger surface. Finger touches the surface of a prism and LEDs provide a light source. Image is captured after its total internal reflection in the prism, by a Charge Coupled Device IC (CCD-IC) or CMOS Camera. Optical sensors are reliable and inexpensive. However they are bulky and prone to surface dirt and dust that affects the quality of fingerprint collected.

b) Capacitive Sensors : These sensors scan surface of finger using *dielectric* measurements to distinguish ridges and valleys. Higher dielectric constant of ridges results in higher capacitance than that of valleys which contain air. Capacitive sensors produce better image quality over wider operating conditions. However they are expensive ,consume more power and also do not work well with dry fingers .

c) Thermal sensors : These sensors consist of contiguous arrangement of heating elements and thermal sensors and capture images based on differentials in *heat emission* between the ridges and valleys. Heat map is converted to an optical image of ridges which are cooler due to presence of sweat pores and valleys which are warmer. Thermal sensors are compact and inexpensive. But they consume more power and are ineffective on warm days.

d) Radio Frequency Sensor : These sensors scan *sub-surface* to get a true image of the finger. They use reflected RF beam to create an image of the layer. RF sensors are not affected by dirt or other impurities , have improved accuracy and reliability .They are also robust and small in size. Also, it is very difficult to fake the finger with this sensor as it takes subsurface image .

Sensor used	Measures	Advantages	Drawbacks	Special Feature
Optical sensor	Visual image	Reliable, inexpensive	Affected by dust, dirt	
Capacitive sensor	Dielectric constant	Better image quality	Expensive, consume more power, not good on dry fingers	
Thermal Sensor	Heat emission	Compact, inexpensive	Consume more Power	Not effective on warm days
Radio Frequency Sensor	Reflected RF beam	High accuracy, compact		Scan subsurface, difficult to fake

Table 1 : comparison of various fingerprint sensors

Fingerprint identification is done using minutiae based matching or pattern matching . In minutiae based matching , the location and orientation of minutiae points are used for matching. The advantage with this method is the small template size typical space required being < 400 bytes per finger . Due to the small template size, matching becomes faster .However the minutiae extraction process itself takes a long time.

In image based matching, the location , orientation as well as a portion of the image around the minutia point is stored . Patches of reference image are placed on test image; each patch is shifted and rotated over the test image to find a best fit .Once all patches are aligned to their best spots , the locations are used to verify the relative distance between patches . Enough patches at the right places indicate a match.

Notable fingerprint biometric systems are i) IAFIS (Integrated Automatic Fingerprint Identification System) maintained by FBI and ii) US-VISIT which confirms whether a person applying for entry/exit from USA is the same person as the one granted visa by the department of state.

2.2 FACE RECOGNITION

Face appearance is a biometric which is used everyday by everyone as a primary means of recognizing other humans[1]. Because of this naturalness it is more acceptable than other biometrics. Face image acquisition is done in the following ways

a) **Single image** : This consists of digital photographs obtained using cameras or scanners.

b) **Video Sequence** : This is obtained from surveillance cameras. However, due to low spatial resolution, it is not very useful for face recognition.

c) **3D Images** : This is based on skin/skull geometry and requires 3D images of the face instead of 2D images . Newer face recognition techniques such as Stereo , structured light and phase based ranging are used for capturing 3D images .[1]

Face recognition approaches in turn are divided into two categories

a) **Face appearance based** : Here, a face image is transformed into what is known as *Eigen faces* .To generate a set of eigenfaces , a large set of digitized images of human faces taken under the same lighting conditions are normalized to line up the eyes and mouths. They are then resampled at the same pixel resolution . Eigenfaces can be extracted out of the image by means of a mathematical tool called PCA (Principal Component Analysis).

b) **Face geometry based** : This is based on face features. Features like the rim of the nose and cheeks of the subject are detected and their geometric relationships are used for recognition of the face as in fig 2.

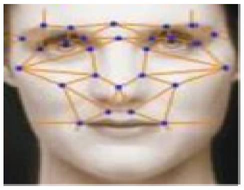


Fig 2 :Geometry based face recognition [16]

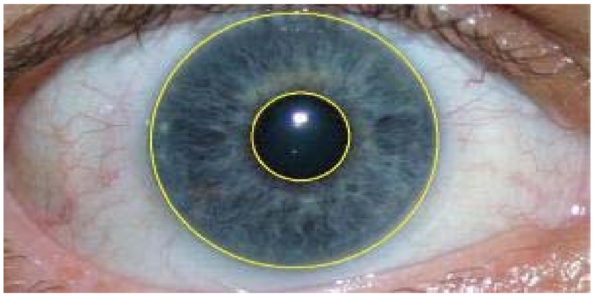


Fig 3 : Iris image [17]

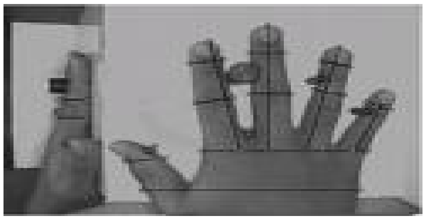


Fig 4 :Hand geometry acquisition device sensing the top and side of hand[18]

Face biometric is implemented by Queensland Transport , Australia for Driver's License with technical support from Unisys Corporation, Sydney. [9]

2.3 IRIS RECOGNITION

The colored part of the eye between he pupil and sclera is called the Iris. Since Iris is a protected internal organ with a complex texture , and because it is unique from person to person and stable throughout life, it forms a very good biometric.

Iris image acquisition is done in two ways

a) **Daugman System** : In this system, an LED based point light source is used along with a standard video camera. The system captures images with the Iris diameter between 100 to 200 pixels from a distance of 15 to 46cm using 330mm lens. John Daugman at the university of Cambridge computer laboratory developed Gabor wavelet based Iris recognition algorithm which is the basis for almost all commercially available Iris recognition systems

b) **Wilde's system** : This system images the Iris with approximately 256 pixels across the diameter from 20cm using 80 mm lens and is area based i.e. it captures the iris as part of a larger image which also contains data derived from the immediately surrounding eye region . [16]

Iris recognition based on John Daugman's algorithms , is used by the United Arab Emirates (UAE) Ministry of Interior for recognizing foreigners entering the UAE , at 35 air, land, and sea ports. Each traveler is compared against about a million Iris codes on a watch-list through internet links ; the time required for an exhaustive search through the database is about 1 second. On an average day, about 12,000 arriving passengers are compared against the entire watch-list i.e. about 12 billion comparisons per day . So far, about 7,500,000 exhaustive searches against that database have been done, making about 7 trillion iris comparisons altogether. A total of 73,180 matches have so far been found between persons seeking re-entry into the UAE and persona non grata on the watch list.[4]

2.4 HAND RECOGNITION

In hand recognition, the geometric features of the hand such as the lengths of fingers and the width of the hand are measured using a charged couple device camera (CCD) and various reflectors and mirrors. Black and white pictures of i) An image of the top of the hand ; and ii) An image of the side of the hand are captured. Unique features in the structure of the hand such as finger thickness, length and width, the distances between finger joints, the hand's overall bone structure, etc are also recorded. To enroll, the user places his or her hand onto a platen three different times ; three images are captured and averaged . The resulting image forms the basis for the enrolment template, which is then stored in the database of the hand geometry scanner. The enrolment phase can be completed within five seconds . In the verification phase, the user is prompted to place his/her hand only once on the platen. An image is captured, and forms the basis for the verification template. The verification template is compared against the enrolment template, in the same fashion as fingerprint recognition. The verification phase can be accomplished in just under one second .This technology is mostly used in physical access entry applications. [5]

2.5 ADDITIONAL BIOMETRICS

a) Retina scan

The retina biometric analyzes the layer of blood vessels located at the back of the eye. This technique uses a low-intensity light source through an optical coupler and scans the unique patterns of the retina's blood vessels . Retina scanning is quite accurate and very unique to each individual similar to the Iris scan; but unlike the Iris scan, it requires the user to look into a receptacle and focus on a given point for the user's retina to be scanned. This is inconvenient for people who wear glasses and those concerned about close contact with the scanning device. This technique is more intrusive than other biometric techniques although the technology itself is very accurate for use in identification, verification and authentication.[9] Additionally, diseases such as cataracts can cause the retina to change making this technique not reliable over a period of time.[11]

b) Vein scan biometric : Vein scan biometric technology identifies a person from the patterns of the blood vessels in the back of the hand. The technology uses near-infrared light to detect vein vessel patterns. Vein patterns are distinctive between twins and even between a person's left and right hand. These are developed before birth, highly stable and change through one's life only in overall size. The technology is not intrusive, and works even if the hand is not clean. It is commercially available and implemented by Fijitsu of Japan[8]

c) Facial thermograph

Facial thermograph detects heat patterns created by the branching of blood vessels and emitted from the skin. An infrared camera is used to capture the resulting images. The advantages of facial thermograph over other biometric technologies are - it is not intrusive, no physical contact is required, every living person presents a usable image, and the image can be collected on the fly. Also, unlike visible light systems, infrared systems work accurately even in dim light or total darkness. Although identification systems using facial thermograms were undertaken in 1997, the effort was suspended because of the cost of manufacturing the system.

d) Skin pattern

The exact composition of all the skin elements such as skin layer thickness, undulations between layers , pigmentation, collagen fibers etc is distinctive to each person. Skin pattern recognition technology measures the characteristic spectrum of an individual's skin. A light sensor illuminates a small patch of skin with a beam of visible and near-infrared light. The light is measured with a spectroscope after being scattered by the skin. The measurements are analyzed, and a distinct optical pattern is extracted.

e) Gait recognition

Recognizing individuals by their distinctive walk, involves capturing a sequence of images to derive and analyze motion characteristics. A person's gait can be hard to disguise because a person's musculature essentially limits the variation of motion, and measuring it requires no contact with the person. However, gait can be disguised if the individual, for example, is wearing loose fitting clothes. Preliminary results have confirmed its potential, but further development is necessary before its performance, limitations, and advantages can be fully assessed.

f) Ear shape recognition

Ear shape recognition is still a research topic. It is based on the distinctive shape of each person's ears and the structure of the largely cartilaginous, projecting portion of the outer ear. Although ear biometrics appears to be promising, no commercial systems are available.[8]

3. PERFORMANCE METRICS

While considering performance measures Biometric systems are classified into verification systems in which a biometric matcher makes a 1:1 match decision based on a score *s* ; and identification systems which makes a 1:m match decision .

3.1 PERFORMANCE METRICS FOR VERIFICATION SYSTEMS :

3.1.1 False Match Rate (FMR) & False Non Match Rate (FNMR)

β and β' be two real world biometrics - say two fingerprints or two faces ; B and B' being the associated machine representations of these biometrics. Then B = f(β) and B' = f(β') where 'f' represents the feature extraction process. However in the real world β and β' are functions of time. Also 'f' is a function of duration of sensing and other environmental factors .This variability is reflected by writing the above equations as $B = B(t) = f_t(\beta(t))$

$B' = B'(t') = f_{t'}(\beta'(t'))$

Biometric match engines , make a decision by computing a measure of the likelihood that the two input samples subject1 and subject2 are the same (but at different times) and therefore that, subject1 (at time t) and subject2 (at time t') are same in real world. This measure called the similarity measure takes β and β' as inputs and computes a score $s(B',B)=s(B'(t'),B(t))= s[f_{t'}(\beta'(t')),f_t(\beta(t))]$

Where B is the enrolled sample's template at time t and is rarely changed and B' is the live query sample's template. Higher is the value of s greater is the likeliness that the two samples come from same person . With this background we use the terms

a) FMR (false match rate) as the proportion of the time that a biometric template B' matches B when β≠β'

$FMR(T)=1-{}_{S=t}\int^{\infty}p_n(s)ds$ where

T is the threshold value of s and $p_n(s)$ is the non match distribution.

b) FNMR(false non match rate) as the proportion of time that a biometric template B' does not match B when β'=β.

A matcher operating at a high threshold T has a low FMR and high FNMR;a low threshold means high FMR and low FNMR.A high False Match / False Accept means security breaches whereas a high False Non Match /False Reject means inconvenience. Hence the threshold T should be selected such that

the biometric system operates in an optimal fashion.

3.1.2 ROC CURVE

The error rates can be plotted against each other as a two dimensional curve called the Receiver Operating Characteristic curve.

ROC(T)=(FMR(T),FNMR(T));

(1,0) as $t \rightarrow -\infty$; (0,1) as $t \rightarrow \infty$

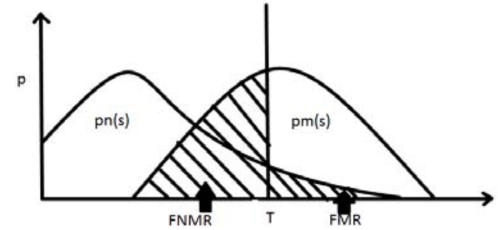


Fig 5. Probability density vs match score curve [1]

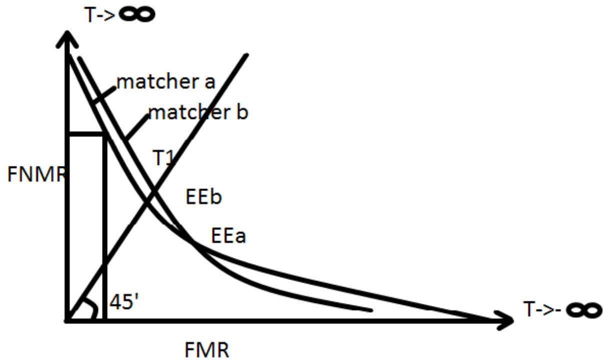


Fig 6 FMR vs. FNMR curve [1]

A point on the ROC curve can be chosen as the threshold and this is called the operating point which specifies the acceptable FMR and FNMR for the biometric system.ROC curve can be used for rating biometric system based on following matrices.

a) Equal error rate : Equal error point is the operating point where FMR = FNMR.For example in figure 6 $EER_a < EER_b$ making 'a' a better system than 'b'. However since this metric is based on a narrow range of operating points, FMR €[EER_a , EER_b] or FNMR €[EER_a , EER_b] ,this forms an unreliable measure of system accuracy.

b) d-prime: Another way of judging the quality of a matcher is to measure how well the non match score probability density $\rho_n(s)$ and the match score probability density $\rho_m(s)$ are separated.

$d' = \mu_m-\mu_n /(\sqrt{(\sigma^2_m+ \sigma^2_n)})$ where

μ_m and σ_m are the mean and variance of matched scores of genuine users.

μ_n and σ_n are the mean and variance of scores of mismatching fingerprints.

c) Expected overall error: Equal error rate and d-prime treat FM and FNM errors as equally likely and of equal importance which is typically not the case for a biometric authentication application. Expected overall error takes into account the possibility of different FM and FNM and is given as

$E(T) = FMR(T)\times\rho_i + FNMR(T)\times\rho_{g.}$ where

T = threshold

ρ_i= probability of a random user being an imposter.

$\rho_{g.}$ = probability of a random user being genuine.

The minimum overall error of a matcher is defined as E_{min} and is the point where ROC intersects a diagonal line L_d from the family $FMR(T)\times\rho_i + FNMR(T)\times\rho_{g.} = K$ with K being the lowest value for such an intersection .

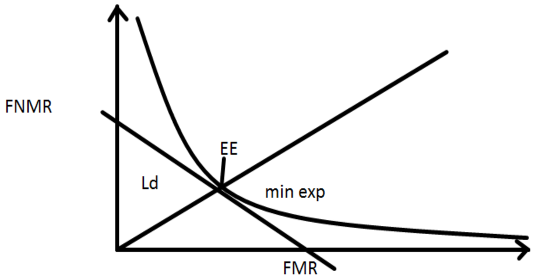


Fig 7. Minimum expected error is not at the same operating point as the equal error rate [1]

d) Cost Functions :

Calculates cost of matcher's decision by associating a cost with each of the errors .

$Cost = C_{FM} \times FMR(T) \times \rho_i + C_{FNM} \times FNMR(T) \times \rho_g$

Cost functions are used in NIST speaker identification evaluation system by putting dolor cost for C_{FM} and $C_{FNM.}$

3.2 PERFORMANCE METRICS FOR IDENTIFICATION SYSTEMS

3.2.1 THRESHOLD BASED IDENTIFICATION

Threshold based identification system compares the query biometric B' to each of the identities in the database , as though that identity had been claimed by the subject in a verification system. This is typically done by computing a score $s(B', B_i)$, i = 1,2,3,…m for each enrolled template and considering all those with scores exceeding some threshold t_0 , as match. The complete list of all matching identities is returned. Following situations are possible :

a) An ideal system which will return m "NO" answers when the test subject is not enrolled or a single "YES" for the correct enrollee when the subject is in the database.

b) More than one candidate may exceed the threshold , giving an ambiguous candidate list and no definite identification .

c) A single false match may exceed the threshold giving a misidentification .

d) No candidate exceeds the threshold even though the text subject is enrolled giving a false reject.

3.2.1.1 FALSE ACCEPT RATE & FALSE REJECT RATE

An imposter is declared as falsely accepted if one or more scores for incorrect candidates exceeds the threshold .The chance of correctly rejecting an imposter is

prob (correct reject) = $_{i=1}\prod^{m}(1-FAR_i)$.

FAR_i = separately measurable FAR for each identity ID_i in database M.

Simplifying FAR_i = FAR(the overall system performance parameter)
Prob(correct reject) = (1-FAR)
Prob of a false accept FAR(m) = 1- prob(correct reject) = 1-$(1\text{-}FAR)^{m.}$
For small FAR , $(1\text{-}FAR)^m \sim 1\text{-}m\times FAR$ Hence FAR(m) = m×FAR
Prob (correct identification) = 1-FRR

3.2.2 RANK BASED IDENTIFICATION

A rank based identification system returns the top 'K' most similar enrolled candidates to the presented biometric B' in some order. Some other secondary decision making process for example a secondary matcher or human operator decides on the actual strength of similarities. Such rank based identification system can do true identification only if

a) The output candidate vector or list is of length one , i.e. , K = 1.

b) Only enrolled users present their biometric to the system . Otherwise if the query biometric B' is not in M, the cases where the rank of correct match is K indicated by L_K.

$L_K = \{B'_l ; r(B_L', B) = K$ ie., when $B_L' = B_K\}$
then $P`(K) = |L_K|/|L|$, K = 1…m

3.2.2.1 CUMULATIVE MATCH CURVE (CMC)

The main issue to be determined for a rank based identification system is –what is the optimal candidate list or vector k. In many cases a fixed k is chosen based on application logistics. For example there might be space on the display screen to show only 8 mug shots with good resolution or there might only be enough human labor available to examine two alternate fingerprints for every passenger screened. To help choose k we use a performance statistic of biometric search engines called the cumulative match curve (CMC).CMC is cumulative sum of RPM $CMC(K) = \sum_{i=1}^{k} P`(i)$ , K = 1…m The expected rank $E(r) = r` = \sum_{k=1}^{m} KP`(K)$ helps evaluate the performance of rank based identification system. K should be > E(r) to give a good chance of finding the correct answer in the candidate list .

candidate list should be empty . In practice , by design , the rank engine is still required to return a list of length K.
A rank based system can only make a misidentification i.e. when the true identity is ranked lower than one or more of the other enrolled candidates. In practice since it is not really possible to guarantee a closed world; performing identification by always taking the highest ranked candidate is not ideal for applications where security is very important.

3.2.2.2 RANK PROBABILITY MASS FUNCTION (RPM) :

The ranking behavior of the identification system can be characterized by the rank probability mass function P(r) defined as P(r) = prob(r) , r = 1…m
For any input query B' corresponding to an enrolled identity ,the probability that the correct identity is ranked in position 'r' is P(r) . The RPM can be estimated empirically as P`(K) , using a database $L = \{B_L , L = 1…L\}$of test biometrics and counting the

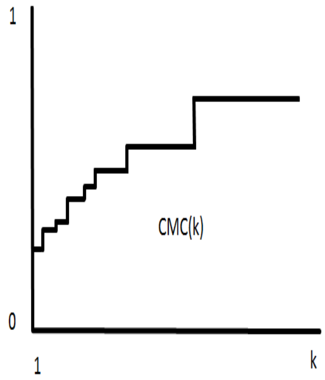


Fig 8. CMC curve [1]

The CMC curve helps us choose k so that the probability that the correct answer is contained in the shortlist is greater than some specified performance goal. The CMC increases with k and when k = m (the whole database) this probability is one .

4. COMPARISON TABLE SUMMARIZING VARIOUS BIOMETRIC SYSTEMS

S.no	Biometric System	Verification	Identification	Accuracy[4]	Reliability[3]	Error Rate	Errors Possible	False Positive	False Negative	Security[3]	Stability[3]	Acceptance[4]	Intrusiveness	Low Cost	Template Size	Transaction Time	Stds Exist?	No of vendors
1	Finger Print	√	√	4	3	1 in 500 +	Dryness,dirt,age	Ext diff	Ext difficult	3	3	2	Some what	√	80-1000bytes	2-10sec	Y	>25
2	Facial Recognition	√	×	3	2	No Data	Lighting,age,glasses, hair	Diffcult	Easy	2	2	2	Non	√	1-4KB	2-10sec	?	7
3	Hand Geom	√	×	3	2	1 in 500	Hand injury, age	Very difficult	Medium	2	2	2	Non	×	9bytes	3-10sec	?	1

	etry																	
4	Iris Scan	√	√	4	3	1 In 131,000	Poor lighting	Very difficult	Very difficult	3	3	2	Non	×	512bytes	10sec	?	1
5	Retinal Scan	√	√	4	3	1 in 10,000,000+	Glasses	Ext difficult	Ext difficult	3	3	2	Very	×		Moderate	?	3
6	Vein Scan	√	×	2	3	No data	-----	Very difficult	Medium	3	3	2	Non	×		Moderate	?	1
7	Facial Thermo gram	√	×	1	2		-----	Very difficult	Medium	3	3	2	Non	×		Moderate	?	1

5. CONCLUSION

The conservative authentication methods are based either on physical possessions of a person like, ID cards , Keys, etc. OR the person's secret knowledge like passwords/ PIN . All these can however be faked with some effort. Also, carrying them may be cumbersome and unsuitable in certain areas of high security / risk zones like military operations. Biometrics emerged as an effective panacea to this serious shortcoming as biological features cannot be faked easily and there is no overhead to be carried or remembered.

A new age of Identity Authentication has thus arrived. Plastic ID cards, paper forms, multiple passwords and pins are slowly but surely making way for the Biometrics.

Research is presently on to combine Biometrics with the emerging revolutionary technology, the nanotechnology the science of altering materials at molecular levels. At this stage, the ideas are still not fully formed, and products are emerging but they will undergo radical changes as nanotechnology starts evolving. Both biometrics and nanotechnology combined could create products too small to be viewed by the human eye. A human being's entire life history could be stored in a chip smaller than a grain of sand. This type technology is under research in the military.

6. REFERENCES

[1] Rudd M.Bolle,Jonathan H.Connell,Sharath Pankanti , Nalini K . Ratha , Andrew W . Senior, Guide to biometrics , Springer Publication (2003).

[2] Davide Maltoni, Anil K. Jain ,Handbook of fingerprint recognition,Springer publication (2002).

[3] Dr. Sujoy Bhattacharya,Consultant (TATA Consultancy Services Ltd.), Digital Image Processing Concepts and Trends Lecture notes

[4] J.G.Daugman,High confidence visual recognition of persons by a test of statistical impedance ,IEEE Transactions on pattern analysis and machine intelligence,15(11):1148-1161,Nov 1993

[5] http://www.findbiometrics.com

[6] http://www.biometricsinfo.org

[7] http://www.biometrics.gov/

[8] Biometrics: Retinal Scanning Amy Zalman

[9] http://www.tiresias.org/

[10] http://www.biovericom.com/biotech/retina.html

[11] www.howstuffworks.com

[12] http://www.globalsecurity.org/security/systems/biometrics-emerging.htm

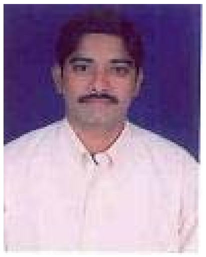
[13] www.authentec.com

7. AUTHORS BIOGRAPHY

Prof J.Ashok is currently working as Professor and Head of Information Technology at Geethanjali College of Engg. & Technology, Hyderabad, A.P, INDIA. He has received his B.E. Degree from Electronics and Communication Engineering from Osmania University and M.E. with specialization in Computer Technology from SRTMU, Nanded, INDIA. His main research interest includes neural networks, data retrieval process and Artificial Intelligence. He has been involved in the organization of a number of conferences and workshops. He has been published more than 30 papers in national and International journals and conferences. He is currently doing his Ph.D from Anna University and is at the end of submission.

Mr. VAKA SHIVASHANKAR is currently working as Asst.professor in Kakatiya College of computer sciences,Warangal,A.P.,INDIA.

He completed his BCA and MCA from Kakatiya University, Warangal,A.P.INDIA. HE is doing M.Tech (CSE) from JNTU. His main research interest includes Artificial Intelligence, Computer Networks, and Data Mining.



Mr.P.V.G.S.Mudiraj is currently working as Associate Professor in the department of MCA at Adams Engg. College ,Paloncha, A.P, INDIA. He received his M.Tech with Specialization in Information Technology from IASE University, Rajasthan He received his MCA from Osmania University, Hyderabad INDIA. His main research interest includes Information Security, data mining and data ware housing and Bio Informatics. Currently he is doing his Ph.D(CSE) from Rayalaseema University