ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 9, September 2016

Analysis of various Bio-metric Techniques

Sanjay G. Galande[1], Dr. G.H. Agrawal[2], Dipali D. Pund[3]

Associate Professor, Dept. of E&TC, Pravara Rural Engineering College, Loni, India[1]

Dean, KDK College of Engineering, Nagpur, India[2]

ME Student, Dept. of E&TC, Pravara Rural Engineering College, Loni, India [3]

ABSTRACT: Biometrics is mechanized methods for recognizing a man or verifying the personality of a man taking into account a physiological or behavioural characteristic has the capacity to dependably recognize an approved individual and a fraud. Since biometric characteristics are particular, can't be forgotten or lost, and the individual to be validated should be physically present at the purpose of recognizable proof, biometrics is characteristically more reliable and more fit than traditional learning based and token-based methods. Using biometrics for recognizing people offers some one of kind focal points. Biometrics can be utilized to recognize you as you. Biometrics holds the guarantee of quick, simple to-use, exact, reliable, and less costly confirmation for a variety of utilizations. This paper gives a review of the distinctive biometric method with a few points of advantages and disadvantages. Than we will attempt to discover which technique is more dependable and secure. The advantage biometric verification gives is the capacity to require more instances of validation in such a quick and simple way that clients are not disturbed by the extra necessities. As biometric advances develop and come into wide-scale business use, managing different levels of verification or numerous instances of validation will turn out to be to a of a burden for clients. Biometrics has been broadly utilized as a part of legal forensics applications, for example, criminal distinguishing proof and jail security, Electronic saving money, e-trade, and get to control. Because of a quick increment in the number and utilization of electronic exchanges, electronic saving money and electronic business are getting to be a standout amongst the most essential developing uses of biometrics.

KEYWORDS: Biometric, False Reject Rate (FRR), False Acceptance Rate (FAR).

I. INTRODUCTION

Biometrics refers to distinguishing an individual in view of his or her physiological or behavioral qualities. Physiological qualities include hand or finger pictures, facial attributes, and iris recognition. Behavioral qualities are characteristics that are found out or obtained. Dynamic signature confirmation, voice check, and keystroke flow. There is nobody “perfect " biometric that fits all needs. All biometric frameworks have their own advantages and disadvantages. There are, be that as it may, some normal characteristics expected to make a biometric framework usable. To start with, the biometric must be based upon a distinguishable characteristic. There is a lot of investigative information supporting "no two fingerprints are alike." Technologies, for example, hand geometry have been utilized for a long time and innovations, for example, face or iris Recognition have come into far reaching use. Some more up to date biometric strategies might be pretty much as exact, however may require more research to build up their uniqueness. Another key perspective is the way "easy to understand" a framework is. The procedure ought to be speedy and simple, for example, having a photo taken by a video camera, talking into a receiver, or touching a unique mark scanner. Ease is critical, yet most implementers comprehend that it is not just the underlying expense of the sensor or the coordinating programming that is included. Regularly, the life-cycle support expense of giving framework organization and an enlistment administrator can overtake the initial expense of the biometric equipment. The physical access control applications have generally utilized token based verification. With the advancement in biometric innovation, these applications will progressively utilize biometrics for authentication. Biometric confirmation requires looking at an enlisted or selected biometric sample (biometric format or identifier) against a recently captured biometric test (for instance, a fingerprint captured during a login). During Enrollment, a sample of the biometric attribute is captured, handled by a PC, and put

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 9, September 2016

away for later examination. Biometric recognition can be utilized as a part of Identification mode, where the biometric framework recognizes a man from the whole selected populace via looking a database for a match construct exclusively in light of the biometric. A framework can likewise be utilized as a part of Verification mode, where the biometric framework validates a man's asserted character from their already enlisted design. This is likewise called "one-to-one" coordinating.

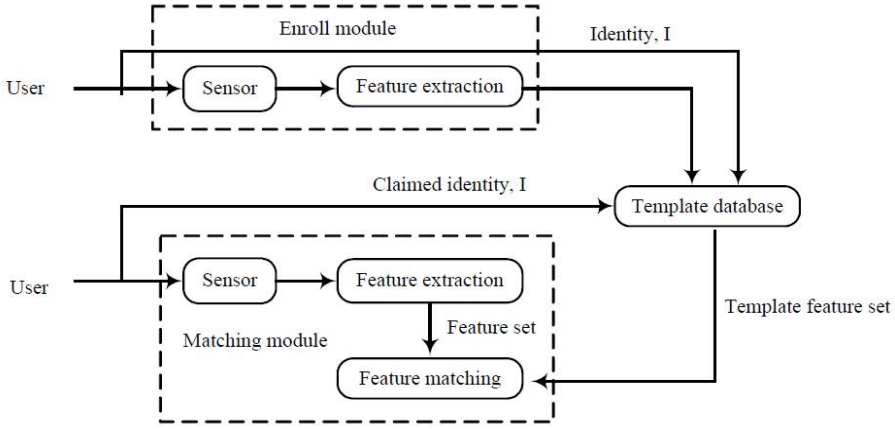


Fig.1 Biometric system

II. TYPES OF BIOMETRICS

A. FACE RECOGNITION

The recognizable of a person of a man by their facial picture should be possible in various different ways for example, by catching a picture of the face in the noticeable range utilizing a cheap camera or by utilizing the infrared examples of facial heat emanation. Facial acknowledgment in visible light ordinarily displays key components from the central portion of a facial picture. Utilizing a wide arrangement of cameras, the visible light frameworks separate elements from the captured image that don't change after some time while maintaining a strategic distance from shallow features, for example, facial expressions or hair. A few ways to deal with demonstrating facial pictures in the noticeable range are Principal Component Analysis, Local Feature Analysis, neural systems, elastic graph theory, and multi-determination investigation. A portion of the difficulties of facial recognition in the visual range incorporate decreases the effect of variable lighting and recognizing a cover or photo. Some facial recognition frameworks may require a stationary or postured client so as to catch the picture, however numerous frameworks utilize a continuous procedure to distinguish a man's head and find the face naturally. Real advantages of facial recognition are that it is non- intrusive, hands-free, and constant and acknowledged by most clients.

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 9, September 2016

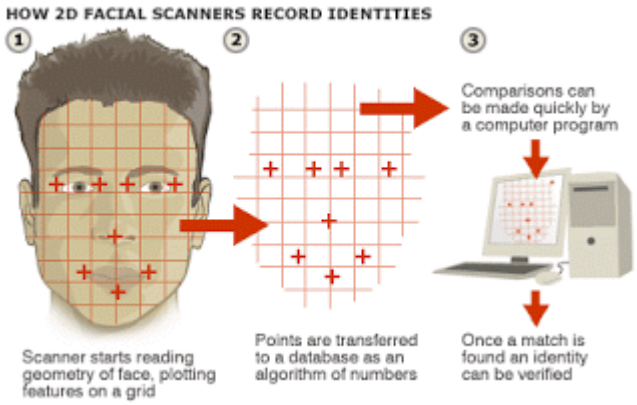
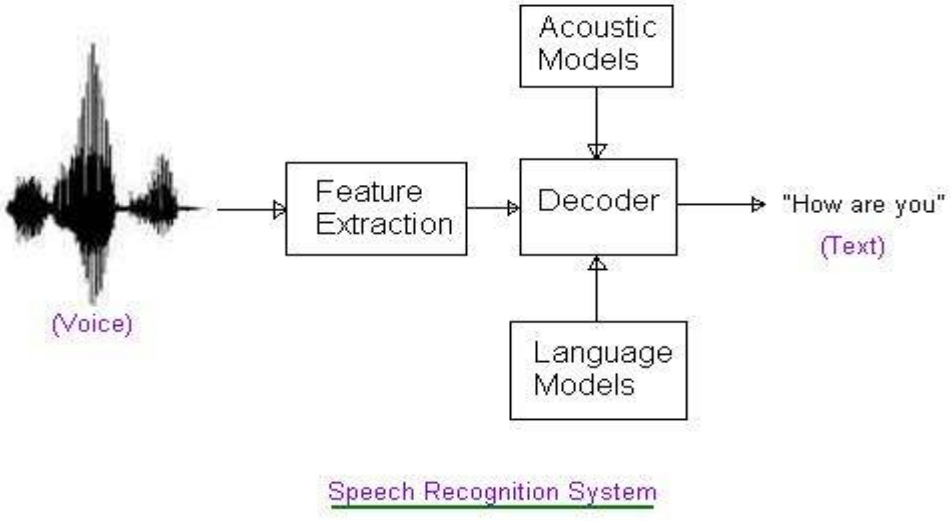


Fig.2.process of face recognition

B. VOICE RECOGNITION

Voice recognition has a history going back somewhere in the range of four decades, where the yield of a few simple channels was arrived at the midpoint of after some time for coordinating. Voice recognition utilizes the acoustic elements of speech that have been found to contrast between people. These acoustic examples reflect both life systems (e.g., size and state of the throat and mouth) and learned behavioral examples (e.g., voice pitch, talking style). This incorporation of scholarly examples into the voice formats (the last called "voiceprints") has earned speaker recognition its characterization as a "behavioral biometric." Voice recognition frameworks utilize three styles of talked information: content text-dependent, text-prompted and text independent. Most voice check applications use text-dependent input, which includes determination and enlistment of one or more voice passwords. Text-prompted is utilized at whatever point there is worry of frauds. The different technologies used to process and store voiceprints include hidden Markov models, design coordinating calculations, neural networks, matrix representation and choice trees. Execution degradation can come about because of changes in behavioral qualities of the voice and from enlistment utilizing one phone and confirmation on another telephone. Voice changes because of maturing likewise should be addressed by recognition frameworks. Numerous organizations market voice recognition motors, regularly as a major aspect of large voice handling, control and exchanging frameworks. Catch of the biometric is seen as non-obtrusive. The innovation needs minimal extra hardware by utilizing existing receivers and voice-transmission innovation permitting recognition over long separations by means of conventional v (wire line or remote).



ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 9, September 2016

Fig. 3. Voice recognition

C. IRIS RECOGNITION

This recognition strategy utilizes the iris of the eye which is the shaded area that surrounds the student. Iris examples are thought unique. The iris examples are acquired through a video-based picture obtaining framework. Iris examining gadgets have been utilized as a part of individual validation applications for quite a long while. Frameworks in light of iris recognition have significantly decreased in cost and this pattern is relied upon to proceed. The innovation functions admirably in both confirmation and recognizable proof modes (in frameworks performing one-to-numerous quests in a database). Current frameworks can be utilized even as a part of the nearness of eyeglasses and contact focal points. The innovation is not intrusive. It doesn't require physical contact with a scanner. Iris recognition has been shown to work with people from various ethnic groups and nationalities

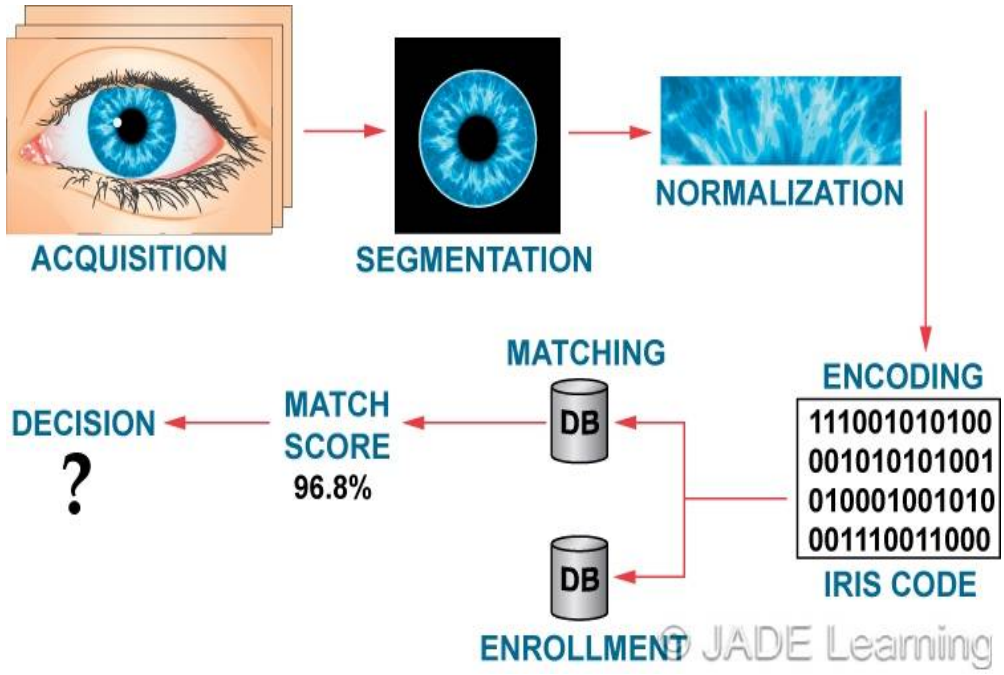


Fig.4 iris recognition

D. HAND AND FINGER GEOMETRY

These techniques for individual validation are established. Hand recognition has been accessible for more than a quarter century. To achieve individual validation, a framework may quantify either physical qualities of the fingers or the hands. These include length, width, thickness and surface range of the hand. One interesting trademark is that a few frameworks require a little biometric test (a couple of bytes). Hand geometry has picked up acceptance in a scope of uses. It can as often as possible be found in physical access control in business and private applications, in time and participation frameworks and when all is said in done individual confirmation applications.

E. SIGNATURE VERIFICATION

This innovation utilizes the dynamic examination of a mark to validate a man. The innovation depends on measuring velocity, weight and point utilized by the individual when a mark is created. One center for this innovation has been e-business applications and different applications where mark is an acknowledged strategy for individual confirmation.

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 9, September 2016

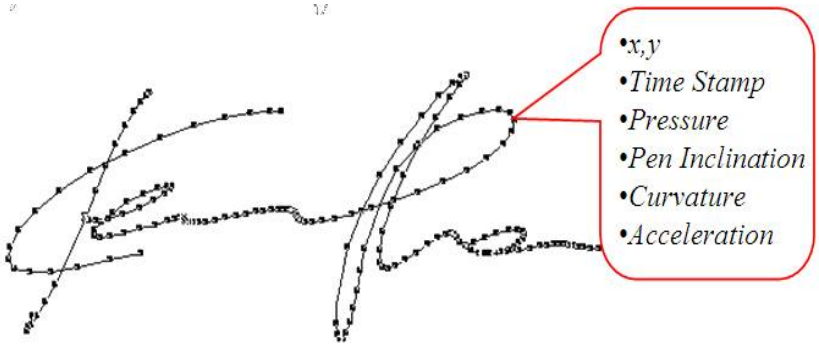


Fig. 5.Signature Verification

F. FINGERPRINTS

The examples of contact edges and valleys on an individual's fingertips are one of a kind to that person. For quite a long time, law implementation has been grouping and deciding personality by matching key purposes of edge endings and bifurcations. Fingerprints are special for every finger of a man including identical twins. A standout amongst the most industrially accessible biometric advances, fingerprint recognition gadgets for desktop and tablet access are presently broadly accessible, clients no more need to type passwords rather, just a touch gives moment access. Fingerprint systems can likewise be utilized as a part of ID mode. A few states check fingerprints for new candidates to social administrations advantages to guarantee beneficiaries don't falsely get benefits under fake names [5]. Fingerprints are the edge and wrinkle designs on the tip of the finger and have been utilized broadly for individual distinguishing proof of individuals. The organic properties of unique mark development are surely knew and fingerprints have been utilized for recognizable proof purposes for quite a long time. Since the start of the twentieth century, fingerprints have been broadly utilized for distinguishing proof of offenders by the different scientific offices around the globe. Because of its criminal intentions, a few people feel uncomfortable in giving their fingerprints to recognizable proof in nonmilitary personnel applications. Be that as it may, since unique mark based biometric frameworks offer positive ID with a high level of certainty, and minimal strong state unique finger impression sensors can be inserted in different frameworks (e.g., PDAs), unique mark based confirmation is turning out to be increasingly well known in various regular citizen and business applications, for example, welfare payment, PDA access, and tablet phone in. The accessibility of shoddy and smaller strong state scanners and in addition vigorous unique mark matchers are two critical variables in the prominence of finger impression based distinguishing proof frameworks. Fingerprints additionally have various burdens when contrasted with different biometric

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 9, September 2016

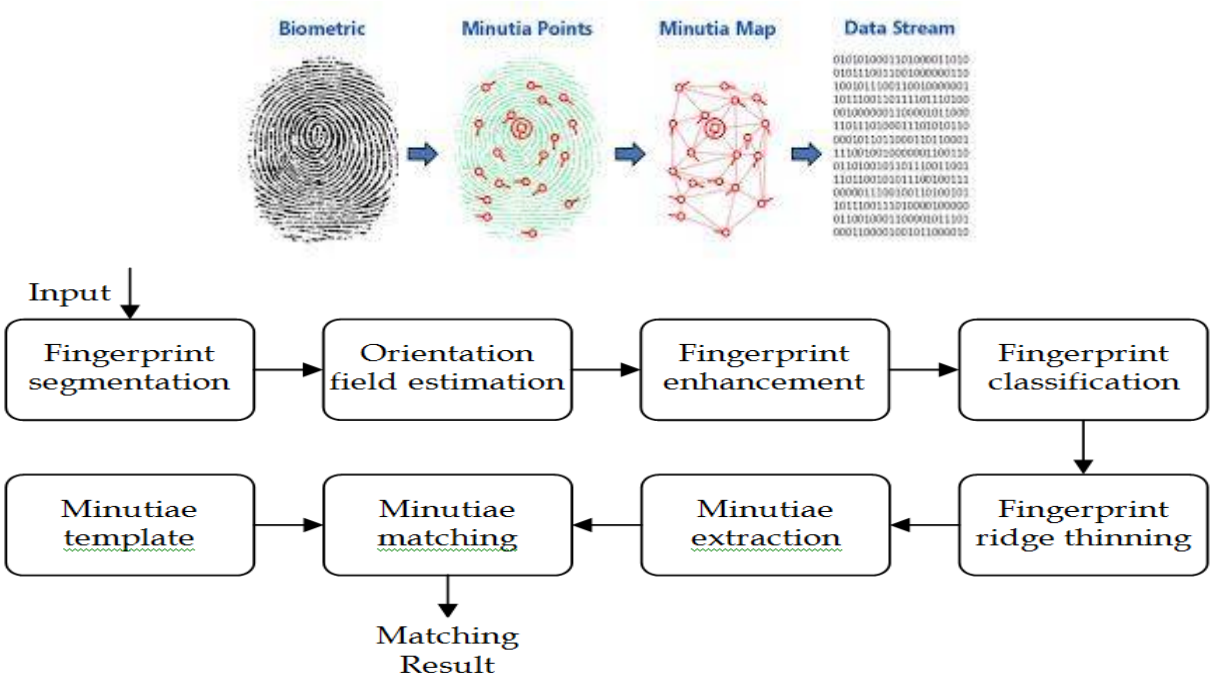


Fig. 6. Process of fingerprint recognition

METHOD	ADVANTAGE	DISADVANTAGE
Finger print Verification	1. High Reliability 2. Robust 3. Highly Distinctive 4. Proven Accuracy 5. Advanced Innovation 6. User Convenience 7. Uniqueness 8. Stable after some time	1. Injury can influence 2. Dry skin can bring about troubles 3. Poor environment
Hand Geometry	Small Template 1. Unaffected by skin Condition	1. Size of Scanner 2. Injury can affect 3. Low Distinctiveness
Face Recognition	1. Efficient Process High Acceptance	1. Face change over time 1. Can be manipulated by surgery 2. Cannot be distinguish between twins 3. Religious or Cultural inhibitions 4. Poor environment
Iris Scanning	Uniqueness 1. Robust 2. Highly Distinctive	1. Complex Processor 2. High Cost 3. Poor environment 4. Relatively new technology 5. Affected with diabetes
Voice Recognition	1. High level of user acceptance	1. Voice and language change 2. over time

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 9, September 2016

	2. High Acceptance 3. Low training requirement	3. Easy to manipulate 4. Low Accuracy 5. Poor environment 6. Flu or Throat infection
Signature Recognition	1. High user acceptance 2. Low training requirement	1. Unstable over time 2. Changes over time 3. Low distinctiveness

Table 1 - advantage and disadvantage of biometric techniques

III. RESULT

Method	False Reject Rate	False Acceptance Rate
Finger print	3 to 7 in 100 (3-7%)	1to10 in 100,000 (.001-.01%)
Face Recognition	10 to 20 in 100 (10-20%)	100 to 1000 in 100,000 (.1-1%)
Voice Recognition	10 to 20 in 100 (10-20%)	2000 to 5000 in 100,000 (2-5%)
Iris	2 to 10 in 100 (2-10%)	>=.001%
Hand Geometry	1 to 2 in 100 (1-2%)	10 to 20 in 1000 (1-2%)
Signature	10 to 20 in 100 (10-20%)	2-5%

Table 2 -Implication of error rates

IV. CONCLUSION

Previously mentioned distinction and implication of mistake rates of various biometric techniques conclude that the unique mark is quick and exact biometric technique for more solid and secure framework.

REFERENCES

[1] George Chellin Chandran. J, Dr. Rajesh. R. S., "Performance Analysis of Multimodal Biometric System Authentication". IJCSNS International Journal of Computer Science and Network Security, VOL.9 No.3, March 2009.
[2] Phillips et al., "*An Introduction to Evaluating Biometric Systems, Guide to Biometrics*", IEEE Computer, February 2000,pp 56-63.
[3] A. K. Jain, A. Ross, and S. Pankanti, "*A Prototype Hand Geometry- Based Verification System*", 2nd Int'l Conference on Audio- and Video-based Biometric Person Authentication, Washington D.C., pp. 166-171, March 22-24, 1999.
[4] Salil Prabhakar, "*Fingerprint classification and matching with filterbank*", Ph.D Thesis, University of Michigan State, 2001.
[5] Robert Carrigan, Ron Milton, Dan Morrow, "*Automated fingerprint identification systems*", Technical Report by Computer world honors case study, 2005
[6] K. Zebbiche, F. Khelifi, and A. Bouridane1, "*An Efficient Watermarking Technique for the Protection of Fingerprint Images*", Hindawi Publishing Corporation EURASIP Journal on Information Security Volume 2008, Article ID 918601, 20 pages.
[7] Tabassam Nawaz, Saim Pervaiz, Arash Korrani, Azhar-Ud-Din, "*Development of Academic Attendence Monitoring System Using Fingerprint Identification*", IJCSNS International Journal of Computer Science and Network Security, VOL.9 No.5, May 2009.