IJCSE International Journal of Computer Sciences and Engineering Open Access

Survey Paper Vol.-7, Special Issue, 6, March 2019 E-ISSN: 2347-2693

# Survey on Recent Trends in Bio Metrics as Authentication

**D. Vinitha[1*], P.V Ramesh[2]**

[1,2]MCA, RIIMS, S V University, Tirupati, India

*Corresponding Author: vinithadivyaraji24@gmail.com Tel.: +91-* 8019936058

DOI: https://doi.org/10.26438/ijcse/v7si6.150153 | Available online at: www.ijcseonline.org

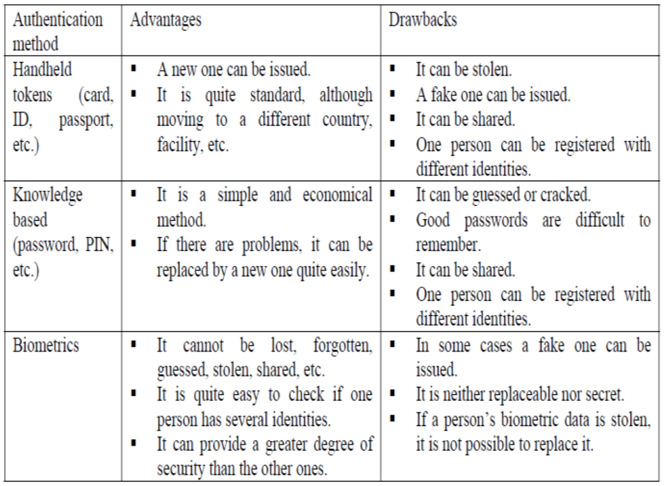
***Abstract***— In this paper, With the raise of rapid innovation in current biometric technology field, new uses are appearing to make the process of authentication more convenient and secure. These innovative and useful processes of human identification are increasing in frequency with every year. As these users are increasing enormously, they are also creating some trends or ways and restructuring the way we identify humans. Passwords can't be used that much extensively as they are easily guessed and prone to guess attacks or brute force attacks. Of all the trends we see in the field of biometric technology, most are focused on finding a better and more efficient way of authenticating a person based on "Who they are." Of course, there are still the traditional ways of identifying a person including personal identification numbers (PINs), ID cards, and passwords but these methods identify a person based on "what they have" or "what they know." Two Factor Security or Multi factor security measures are quite applicable to some of the domains / ideas. None of them identifies a person with the most important factor, which is "Who they are." As biometric traits are personal and unique, this is perhaps the most accurate way of identifying a person.

***keywords— Biometrics, Two Factor Security, Authentication, Iris Scan, Palm Vein Technologies.***

## I. INTRODUCTION

The word Biometrics comes from the Greek words "bios" (life) and "metrikos" (measure). Frankly speaking, it refers to a science involving the statistical analysis and observation of biological characteristics. Thus, we should refer to biometric recognition of people, as those security applications that analyze human characteristics for identity verification or identification. We will use the short term "biometrics" to refer to "biometric recognition of people". Biometric recognition offers a promising approach for security applications, with some advantages over the classical methods, depends on something you have (key, card, etc.), or something you know (password, PIN, etc.). These methods requires something either password or some token has to be remembered. Authentication methods by means of biometrics are a specific portion of security systems, with a good number of advantages over classical methods. A good Biometric system must possess the following properties:

Universality: Each person should have some identification that is unique. Acceptability: acceptance should be taken from the user that this technique is not annoying and should be convinced in its usage, and educating towards its importance. The performance something like the time required to authenticate using the underlying technique or Biometric system should be reasonably good. Circumvention is the concept of fraudulent users in identifying their fooling activities should be defended. Collectability the idea should be accountable and quantifiable. Distinctiveness: is the idea of differentiating multiple users with their attributes. These traits can be divided into two categories: Physiological and Behavioral. Physiological things refer to fingerprint, iris, face and hand-scan recognition. Behavioral traits covers signature, gestures, key stroking recognition. For example if we take speech trait then the parameters that are needed to be considered are diction, speech. Biometrics can be operated in two modes: Identification and Verification



| Authentication method | Advantages | Drawbacks |
|---|---|---|
| Handheld tokens (card, ID, passport, etc.) | ▪ A new one can be issued.<br>▪ It is quite standard, although moving to a different country, facility, etc. | ▪ It can be stolen.<br>▪ A fake one can be issued.<br>▪ It can be shared.<br>▪ One person can be registered with different identities. |
| Knowledge based (password, PIN, etc.) | ▪ It is a simple and economical method.<br>▪ If there are problems, it can be replaced by a new one quite easily. | ▪ It can be guessed or cracked.<br>▪ Good passwords are difficult to remember.<br>▪ It can be shared.<br>▪ One person can be registered with different identities. |
| Biometrics | ▪ It cannot be lost, forgotten, guessed, stolen, shared, etc.<br>▪ It is quite easy to check if one person has several identities.<br>▪ It can provide a greater degree of security than the other ones. | ▪ In some cases a fake one can be issued.<br>▪ It is neither replaceable nor secret.<br>▪ If a person's biometric data is stolen, it is not possible to replace it. |

Fig. 1

In this verification approach the systems goal is to determine whether the person is the right one or not based on his claim. This operation is called as detection or authentication. The performance of the system can be assessed or evaluated using FAR (False acceptance Rate) also known as False Alarm and False Rejection Rate (FRR) also known as Miss in Detection Theory. This operations and results can be plotted as a ROC Curve (Receiver Operating Characteristic) Curve or a DET Curve. (Detection error trade-off curve).

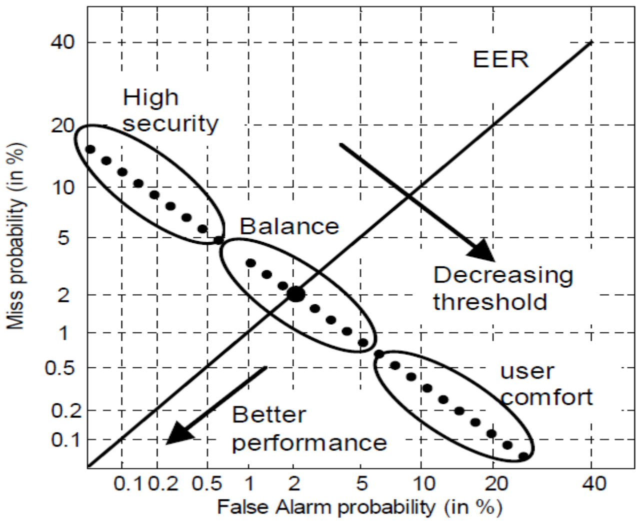


Fig. 2

The above figure shows a DET Curve which has two lines one line is EER Curve and other one is high security and the intersection point is called Balanced performance. The same is also explained using ROC (Receiver Operating Characteristic) Curve. Decreasing Threshold can be may increase the users comfort. Increasing Threshold may produce High Security.

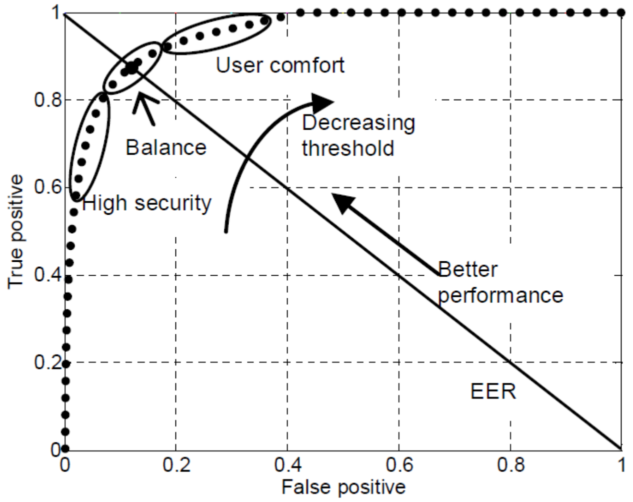


Fig. 3

## II. Related Work

The Fingerprint can be Ink + Paper + Scanner, optical, capacitive, Ultra Sound, Photo- Camera these are the several ways of fingerprint analysis. For Face Recognition video camera is used. For enabling speech recognition microphone is used. For Iris recognition Kiosks, physical access devices and webcams of PCs. Retina Scanner is used for scanning Retina. Signature recognition can be done by Ball Pen + Paper + Scanner , Graphics Tablet, PDA. Hand- geometry can be recognized by Hand Scanning device, conventional scanner, and conventional camera, palm print can be done by Document-Scanner, Keystore analysis can be done by keyboard.

Table 1

| **Biometric Trait** | **Sensor** | **Comments** |
|---|---|---|
| Finger Print | Ink + Paper + Scanner | Conventional or oldest |
| | Optical | Easy to operate but with some distortions |
| | Capacitive | More difficult to operate than optical |
| | Ultra Sound | Maintenance Cost |
| Face | Photo-Camera | High resolutions and quality |
| | Video-Camera | Smaller Resolutions |
| Speech | Micro-Phone | Low-cost, easy-to-operate |
| Iris | Kiosk based Systems | Camera searches for eye position |
| | Physical access devices | Device requires some user efforts |
| | Desktop Cameras | Cheap but difficult to use |
| Retina | Retina-Scanner | Image acquisition is not a trivial matter |
| Signature | Ball Pen + Scanner | Off-line |
| | Graphics tablet | Safer stylus is needed |
| | PDA | Some potential Applications |
| Hand-geometry | Hand-Scanning Device | Prices are high |
| | Conventional Scanner | Hand profile is needed |
| | Conventional Camera | Faster |
| Palm-print | Document Scanner | Conventional Document Scanner |
| Key stroke | Keyboard | Standard keyboard |

## III. METHODOLOGY

The Sensor is the basic unit for gathering any data. This sensor could be PDA, Scanner, Graphics Tablet, Optical Scanner etc., is used to get the input in digital format. Later this format can be used to extract the features of the Scanned or sensed data or image. Matching these with the under database that is stored as several models, if there is a match then the decision maker will come into play. Decision maker is going to take the decision.

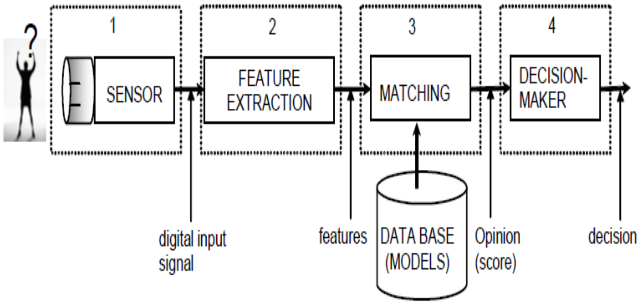


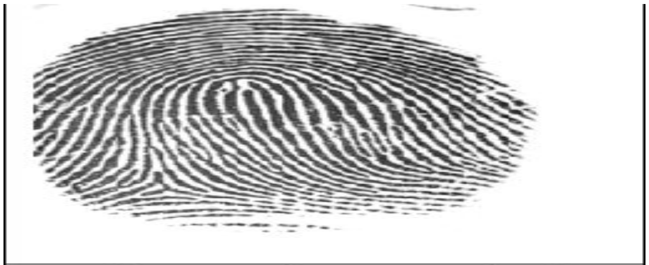
Fig. 4

The following are some snaps of images taken by the sensor or sensing unit.

Graphics tablet for signature

Fig. 5

Here the graphical tablet is used for grabbing or scanning signature written by Stylus.



Fingerprint Acquired with optical sensor

Fig. 6

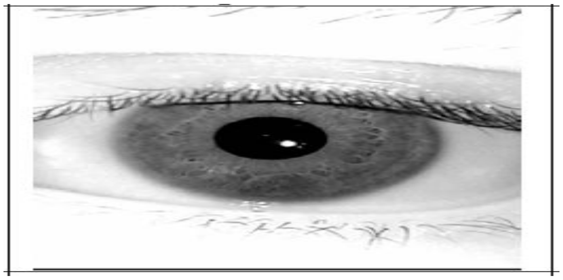


Fig.7. Iris Scanner

2D Hand geometry acquired with a document scanner

Fig. 8

Fingerprint optical scanner

Fig. 9

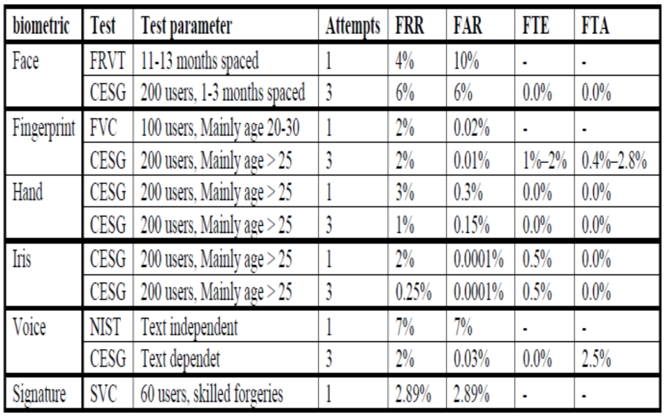
Webcam

Fig. 10

## IV. RESULTS AND DISCUSSION

Here are results of some studies, such as FVRT (Face Recognition Vendor Test), CESG (Communications

Electronics Security Group), FVC (Fingerprint Verification Competition) and NIST (National Institute of standard technologies), and SVC (Signature Verification Competition). This table is an update of [26]. A nice property of CESG evaluation is that all the results have been obtained with the same set of 200 users.



| biometric | Test | Test parameter | Attempts | FRR | FAR | FTE | FTA |
|---|---|---|---|---|---|---|---|
| Face | FRVT | 11-13 months spaced | 1 | 4% | 10% | - | - |
| | CESG | 200 users, 1-3 months spaced | 3 | 6% | 6% | 0.0% | 0.0% |
| Fingerprint | FVC | 100 users, Mainly age 20-30 | 1 | 2% | 0.02% | - | - |
| | CESG | 200 users, Mainly age > 25 | 3 | 2% | 0.01% | 1%–2% | 0.4%–2.8% |
| Hand | CESG | 200 users, Mainly age > 25 | 1 | 3% | 0.3% | 0.0% | 0.0% |
| | CESG | 200 users, Mainly age > 25 | 3 | 1% | 0.15% | 0.0% | 0.0% |
| Iris | CESG | 200 users, Mainly age > 25 | 1 | 2% | 0.0001% | 0.5% | 0.0% |
| | CESG | 200 users, Mainly age > 25 | 3 | 0.25% | 0.0001% | 0.5% | 0.0% |
| Voice | NIST | Text independent | 1 | 7% | 7% | - | - |
| | CESG | Text dependet | 3 | 2% | 0.03% | 0.0% | 2.5% |
| Signature | SVC | 60 users, skilled forgeries | 1 | 2.89% | 2.89% | - | - |

Fig. 11

## V. CONCLUSION AND FUTURE SCOPE

There is a huge enhancement and comfort related to this as per as Security and Privacy are concerned. But Privacy is not that much assured with this Bio-Metric devices. Even though Biometrics are a solution to the weak passwords but privacy is not assured. Some kind of liveliness detections are needed so as to avoid privacy attacks should be provided. Anti-Replay attacks should also be adapted so as to ensure privacy of this Biometrics.

## REFERENCES

[1] R. Clarke "Human identification in information systems: management challenges and public information issues". December 1994. Available in http://www.anu.edu.au/people/Roger.Clarke/DV/HumanID.html

[2] S. Furui *Digital Speech Processing, synthesis, and recognition*., Marcel Dekker, 1989.

[3] A. Martin, G. Doddington, T. Kamm, M. Ordowski, and M. Przybocki, "The DET curve in assessment of detection performance", V. 4, pp.1895-1898, European speech Processing Conference Eurospeech 1997

[4] A. J. Mansfield, J. L. Wayman, "Best Practices in Testing and Reporting Performance of Biometric Devices". Version 2.01. National Physical Laboratory Report CMSC 14/02. August 2002.

[5] M. Faundez-Zanuy "Door-opening system using a low-cost fingerprint scanner and a PC". IEEE Aerospace and Electronic Systems Magazine. Vol. 19 nº 8, pp.23-26. August 2004

[6] M. Faundez-Zanuy y Joan Fabregas "Testing report of a fingerprint-based door-opening system". IEEE Aerospace and Electronic Systems Magazine Vol.20 nº 6, pp 18-20, ISSN: 0885-8985. June 2005..

[7] D. Maltoni, D. Maio, A. K. Jain, S. Prabhakar "Handbook of Fingerprint Recognition" Springer professional computing. 2003

[8] M. Faundez-Zanuy "Technological evaluation of two AFIS systems" IEEE Aerospace and Electronic Systems Magazine Vol.20 nº 4, pp13-17, ISSN: 0885-8985. April 2005.

[9] M. Faundez-Zanuy "Are Inkless fingerprint sensors suitable for mobile use? IEEE Aerospace and Electronic Systems Magazine, pp.17-21, April 2004

[10] S. Prabhakar, S. Pankanti, A. K. Jain "Biometric recognition: security and privacy concerns" IEEE Security
and Privacy, pp. 33-42, March/April 2003

[11] M. Faundez-Zanuy "On the vulnerability of biometric security systems" IEEE Aerospace and Electronic Systems Magazine Vol.19 nº 6, pp.3-8, June 2004

[12] M. Faundez-Zanuy "Data fusion in biometrics". IEEE Aerospace and Electronic Systems Magazine. Vol. 20 nº 1, pp.34-38, January 2005

[13] http://www.faceblind.org/research

[14] http://www.rarediseases.org

[15] S.K. Zhou "Face recognition using more than one still image: what is more?. Lecture Notes In Computer Science LNCS 3338, pp.212-223, A. Z. Li et al. Ed., Sinobiometrics. Springer Verlag 2004

[16] M. Faundez-Zanuy, V. Espinosa-Duró, J. A. Ortega-Redondo "Face verification by means of a single Neural Network classifier". Enviado a IWANN'05. Lecture Notes In Computer Science 2005

[17] M. Faundez-Zanuy, E. Monte-Moreno "State-of-the-art in speaker recognition". IEEE Aerospace and Electronic Systems Magazine. Vol.20 nº 5, pp 7-12, ISSN: 0885-8985. May 2005

[18] Marcos Faundez-Zanuy, G. Mar Navarro-Mérida "Biometric identification by means of hand geometry and a neural net classifier" "IWANN'05 Lecture Notes In Computer Science 2005

[19] P. W. Hallian "Recognizing human eyes" Geometric methods computer vision, vol. 1570, pp. 214-216, 1991.

[20] M. Faundez-Zanuy "Signature recognition state-of-the-art". IEEE Aerospace and Electronic Systems
Magazine. 2005. Vol.20 nº 7, pp 28-32, ISSN: 0885-8985. July 2005.

[21] P. J. Phillips, P. Grother, R. J. Micheals, D. M. Blackburn, E. Tabassi, and J. M. Bone "FRVT 2002: Evaluation report", available online: http://www.frvt.org/DLs/FRVT_2002_Evaluation_Report.pdf, March 2003

[22] T. Mansfield, G. Kelly, D. Chandler, and J. Kane (2001, Mar.) biometric product testing final report.

[23] D. Maio, D. Maltoni, R. Capelli, J. L. Wayman, and A. K. Jain "FVC2000: fingerprint verification competition". IEEE Trans. Pattern analysis Machine Intelligence, Vol. 24, pp. 402-412, march 2002

[24] A. Martin and M. Przybocki, "The NIST 1999 speaker recognition evaluation: An overview". Digital signal processing Vol. 10, no.1-3, pp.1-18, 2000.

[25] D. Yeung, H. Chang, Y. Xiong, S. George, R. Kashi, T. Matsumoto and G. Rigoll "SVC2004: First international signature verification competition". Lecture Notes on Computer Science LNCS-3072, Springer Verlag pp.16-22, 2004.

[26] L. O'Gorman "Comparing passwords, tokens and biometrics for user authentication". Proceedings of the IEEE, Vol. 91, No. 12, pp.2021-2040, December 2003.

[27] M. Faundez-Zanuy "Biometric recognition: why not massively adopted yet?". IEEE Aerospace and Electronic Systems Magazine. Vol.20 nº 8, pp.25-28, ISSN: 0885-8985. August 2005.

[28] M. Faundez-Zanuy "Privacy issues on biometric systems". IEEE Aerospace and Electronic Systems Magazine. Vol. 20 nº 2, pp13-15, February 2005.

## Authors Profile

Ms D.Vinitha, Studying Master of Computer Application of Rayalaseema Institute of information and management sciences.

Mr.P.V .Ramesh,Asst.Professor of Rayalaseema Institute of information and management sciences.