International Journal of Innovative Research in Science, Engineering and Technology (IJIRSET)

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512|

||Volume 9, Issue 5, May 2020||

A Comparative Study and Analysis on Biometric Authentication

Rohit Chauhan[1] , Krishan Kumar[2]

PG Student, Department of Computer Science, Amity University, Gurugram, India[1]

Assistant Professor, Department of Computer Science, Amity University, Gurugram, India [2]

ABSTRACT: According to Biometric states to the metric linked to the human appearance. It is accurate verification which is used for proof of identity and entree control. Biometric is as well as used for recognize the individuals features used for tag and define individuals. The Biometric Authenticator's are commonly label as Physiological as well as Behavioural Features. The Physiological features are linked to the outline of the Figure or body. By operating biometrics a user could be illustrious in the view of "who he/she is " in it's place of "what he/she has" (postcard, mark, scratch) or "what he/she tells" (Password, Pin). In this review paper mainly we focused on the biometric and their application which we used in our daily life.

KEYWORDS: Verification, Biometric, Challenges, Authentication, Privacy, Recognition.

I. INTRODUCTION

The Biometric authentication is quick, exact and human friendly tool which offers an effective and consistent solution in the multiple access control system. With the fast advancement of the internet and moveable device(Mobile), authentication framework have been broadly utilized in the web access and cell phone access for ensuring client gadgets, substance, and accounts. At the point when clients hold an lot ofaccounts, remembering the password of these accounts is very difficult it's very big issue,particularly those with high security levels. So as to take care of this issue, biometrics were contemplated and applied in different authentication because of their extraordinary or unique attributes.

Researchershaveshownwide and in-depth study on biometric confirmation in current years. Some scholarsintensiveon the specificprocesses or outlines used in biometric built authentication.Kannavara and Bourbakis[1]concise a sequence of biometric recognition proceduresbuilt on neural grids by viaspeech, face, palm, iris, fingerprint and pointy out possible ways to expand these procedures. Shunmugam and Selvakumar[2] supposed that unimodal biometric procedures are restricted. Multimodal biometric approaches are much more consistent for structure up ainnocuous verification structure. They debated multi modalapproaches as manysensor,severalalgorithms,severalexamples, severalmodels and mixture models.

This paper is divided into some sections as follow: Section2 contains the "Types ofBiometric"Which is further divided into two parts physiological and behavioural biometric. Further they are also divided into some parts like Face recognition, Fingerprint, Iris, Palmprint, Speech, Keystroke, Signaturebiometricsverification systems, analyse its probable privacy and security threats. In Section 3, we discussed about the challenges in biometric verification systems in a table form. Section 4 we discussed about conclusion.

II. LITERATURE REVIEW

The survey of biometric, we studied last few years published paper byieee digital library, amc digital library, different journals, articles on biometric and we reviewed the works on biometric in the paper. The key-words we mainly used in the paper like authentication, biometric, verification, face, privacy, fingerprint, detection and so on. We studied the biometric is further divided in to sub parts. The first sub part of biometric is based on static feature which is know as physical characteristic of human. It is also known as physiological biometrics. Such as fingerprint, face, iris and so on. The second part of biometric is based on dynamic feature that is biological biometric. It contains such as signature, voice, keystroke and so on. Basically, the biometric word contains two word "bios" and "metrikos". Bios means "life" and Metrikos means "measure". Basically, it comes from Greek language. There are lot of researches has been done on biometric. Every researcher said something new about biometric. In face recognition there is very deep research result in it. Gonzalez-jimenez and Alba-Castro[10] gave a very deep dispersal model to easily agreementthrough the different-different position of the face in 2-Dimension face identification. They used position parameters to produce positionmodified pictures based on tinny platterfinsconstructed warping. Thavalengal et al. [11] He find the option of

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512|

||Volume 9, Issue 5, May 2020||

iris verification applied to those device which is non-contact handheld. He claimedthat the pixel determination or resolution still bounds the application of iris verification, althoughpresentophthalmic design and smartphone volume can't agree the embedment of the structure.Kot and Li[6] gave a system which have authentication is fingerprint based. That system uses data embedding and data hiding technology to convert user's private data into the templates of fingerprint. Basically the identity of user is hidden in that templates which is safely stored in database. That templates stored in bases on binary pattern on hefinger which is collected by fingerprint sensor. The information of user can't stolenby attackers because of data hiding technique.

Now the days fingerprint is consider as one of the oldest and popular among other biometric technique. Palm verificationis that method which equating the dual example of rubbingedgecoatingimprint from the user finger, toe, or palm[12].

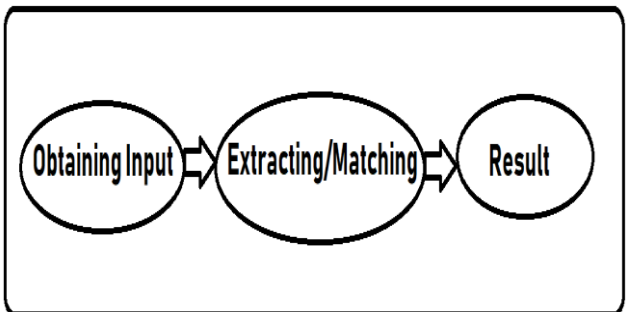


Fig 1 Basic Structure of Biometric Process

Due to low rate of forgery the finger vein biometric verification system is secure and quick rather than all biometric technique told byNerkar and Jadhav[8]. They gave a algorithm which is image or photo processing algorithm. They found that the fingerprint template matching accuracy is 97 % .

Maltoni and Franco were gave a research paper in which they were focused on the bogus fingerprint verification. Mainly they were also focused on reverse engineering. Both researchers thought that the by using of reverse engineering the hacker hack or forge the fingerprint. Thus hackers will access the private information of user and make a fake access in authentication system[9].

III. TYPES OF BIOMETRIC

Biometric is further divided into two parts

1. Physiological Biometric
2. Behavioural Biometric

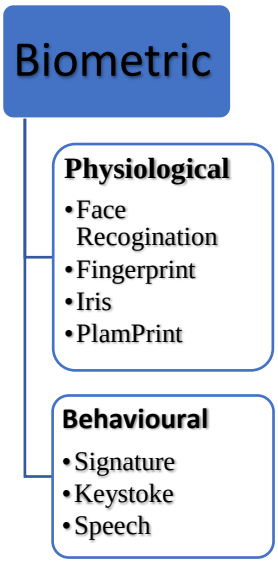


Fig.2 Types of Biometric

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512|

||Volume 9, Issue 5, May 2020||

A.Face Recognition

Face Recognition is a technique which is used for identification of the people's.Basically the face detection technique is works on Nodal Points. Nodal points are the endpointsby which camera or sensor done the measurement of points on the face foridentification of the person. The face recognition technique also measure the width and length of a nose, the shape and size of the lips and the size of cheekbones of the person.Aentire face recognition erectionholds two typesof face recognition and face detection. In the biological structuresof the face havefull structurallikeness and different local variances[3].Consequently it isessential to excerptthe basicstructures of the expressionby theexpression detection process and to isolated the faces from the relatedoutline and face recognition of the divided faces. This is a method of miningcontrolled face pictures, and then differenceandproof of identity, the resolutionis todecide the character of the face from the pictures.

B.Fingerprint

Fingerprint based verification systems have been broadly accepted in both academic world and business or industry. Fingerprint recognition states to the automatic process of classifying or confirming the uniqueness of an distinct built on the judgement of two fingerprints. Fingerprint works on Minutiae. Minutiae denote to exact points in a fingerprint. Minutia is separated in to two portions such as: termination and bifurcation. Termination is also known as finish point and bifurcation is also called branch.

Fig3 Fingerprint Process

C. Iris

In the iris recognition it grew a boundless devotion various ground like business area, security area, boundary area and health institutes etc. From it's high correctness and uniqueness, it is used in several fields of entrée control and safety at border ranges. The request for iris verification is increase very highly in the day to day life due to it's consistency, correctness and uniqueness. The coloured circle in our eye around the pupil is called iris. It's baroque pattern is unique. It has attained a excessive devotion in previous years due to it's inimitable features such as edges, spots, furrows, rings and multipartshape and thus it position a great degree of chance.

D.Palm Print Recognition

The Hand Geometry is dealing with the outline of the palm. This tech offers minor pattern or template size(9-25byte) and min storage desires. Feature mining is comparatively simple, so the minimum cost processor will use. In accumulation, it is probably to complete a hand-print recognition, which can take benefit of the internal surface among wrist and finger off a human. This area offering rich data, including lines and ridges/valley like to a fingerprint, but in greater surface. While there are not viable system via hand-prints, some trails have been achieved at college using this info alone and shared with the palm geometry for better quality and better accuracy. It measures the hands size, shape and palm print by the various point as I shown in figure 1.4.

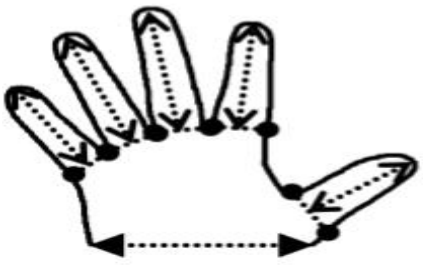


Fig4 Palm Print [7]

E. Signature

The Signature is possibly very most believed process for recognize. We normally usesignaturewhen adoption glory Cards receipts, forms etc. In adding, biometric offerings a very serious weakness when equated with standard procedures of password and marks(it is probable to get a new id number, itcan't replace any biometric information, which must last endlessly) [5]. Though, Signature isallowance, because handler can change his signature. While,

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512|

||Volume 9, Issue 5, May 2020||

hypothetically, a user could study to sign in closely the similarmeans another user, in training, it is so much tough to duplicate the dynamicinfofor every digitized signature fact(pixels) which can't belearnt frominvestigative a written.

Fig5 Signature[4]

F.Keystroke

Keystroke is basically recording or taking/capturing the hits on a keystroke to monitoring the peoples. That is the behaviour of the Person or human. It Means the dissimilarperson have the dissimilar technique of press the button or key onthe basic identification takings Place. Keystrokeis the hundred percent constructed, needing no sensor more than computer.

G. Speech

The phone system offers a global system of sensors for obtaining speech indicators. Also for non-microphone application, microphone are minimum cost, it is calm to work. And willingly available. The Speech signals can be obtain easily. Through, one of the serious facts for speaker recognition is the occurrence of station changeability from training to testing, that is, dissimilar signal to sound ratio kind of microphone, development with time etc. It is not a thoughtful problem for people because it uses the different level of information. Through. This disturbs instinctive system in a important manner. Fortunately, advanced level signals will notaffected by noise and channel mismatch. Few examples of higher level info in the speech signals are the pause and speaking percentage, pitch and effectiveness patterns, individual phrase/word usage, different pronunciations etc. Present system effort to take benefit of these different levels.

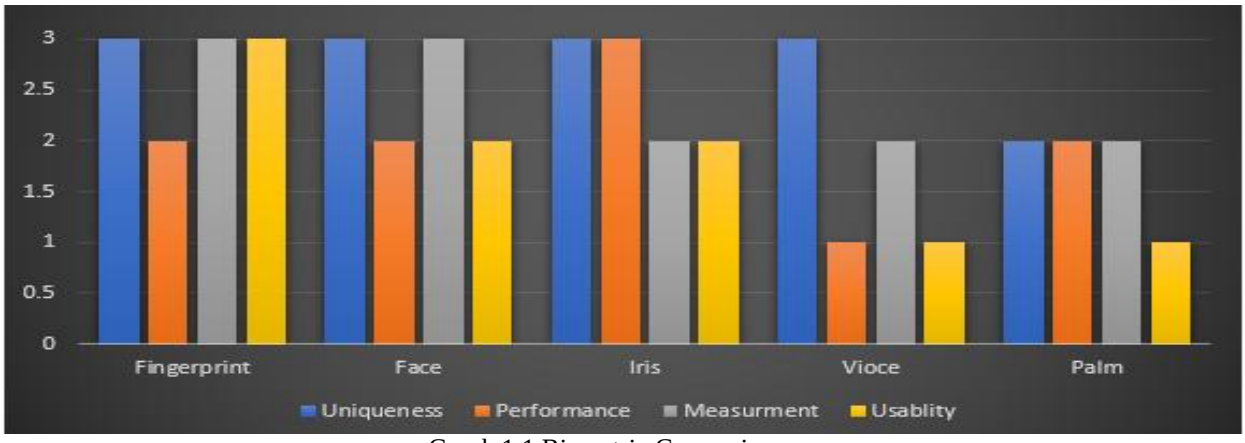
IV.**RESULTS**

In this paper I talk about the biometric and types of biometric. How biometric works. I compare biometric according to usability, security etc in a graph. I found some challenges in every biometric technique.

S.No	Biometric Technique	Challenges
1	Face Recognition	• Rotation in face • Variation in light(low or high light on face) • User wearing collusion (Eye glass, hat, scrap)
2	Fingerprint	• If finger is wet and winkled finger
3	Iris	• If eye is covered by occlusion. Eye glass, Contact lenses, Watery eye.
4	Palm	• If your palm is wrinkled or wet so it is also a big challenge to identification.
5	Signature	• Long time consistency, price and lack of correctness are the core problems to be addressed in that technology.
6	Keystroke	• Key pressing speed • Time between pressing and releasing the key

7	Speech	• Low or High voice • Person Sick or Emotional voice • Person's voice in anger

Table 1 Challenges in Biometric



Graph 1.1 Biometric Comparison

V. CONCLUSION

In conclusion ofreview paper i revised the current advance in the area of biometricverification.Ipoint out possiblesecurity risk and attacksin the biometricverification andadditionallyplanned thesequence of assessmentprinciples for assessing the presentation of current works.I provide a relativeassessment on the current literature byseparatingpresent the biometricverification systems into two typesdynamic biometric or static biometric. We originate that the existing systems serves from privacyand securityproblems, although the verificationcorrectnessof the system should further improve on dynamic biometric. Bases on our survey we find many open problems andpredictionupcoming research directions. We trust that the improving the privacy and security of biometric verification should be highlighted future research.

REFERENCES

[1] E. M.-Tzanakou, N. V. Boulgouris and K. N. Plataniotis, Ed., "A comparative survey on biometric identity authentication techniques based on neural networks".IEEE 2009, ch 3,pp 47-79.
[2] S. Shunmugam, Z. Wang, E. Wang, and S. Wang, "Electronic Transaction Authentication- A survey on Multimodal Biometrics," pp. 1–4, 2014.
[3] Y. Sun, X. Wang, and X. Tang, "Deep Learning Face Representation from Predicting 10 , 000 Classes."
[4] S. A. Sahmoud and I. S. Abuhaiba, "Ef fi cient iris segmentation method in unconstrained environments," Pattern Recognit., vol. 46, no. 12, pp. 3174–3185, 2013, doi: 10.1016/j.patcog.2013.06.004.
[5] M. Fatindez-zanuy, "On the Vulnerability of Biometric Security Systems," no. June, pp. 3–8, 2004.
[6] S. Li, S. Member, and A. C. Kot, "Fingerprint Combination for Privacy Protection," vol. 8, no. 2, pp. 350–360, 2013.
[7] K. Dharavath, F. A. Talukdar, and R. H. Laskar, "Study on biometric authentication systems, challenges and future trends: A review," in 2013 IEEE International Conference on Computational Intelligence and Computing Research, IEEE ICCIC 2013, 2013, doi: 10.1109/ICCIC.2013.6724278.
[8] M. Jadhav, "Implementation of an Embedded Hardware of FVRS on FPGA," pp. 48–53, 2015.
[9] A. Franco and D. Maltoni, "Fingerprint Synthesis and Spoof Detection," pp. 2002–2003.
[10] D. González-jiménez and J. L. Alba-castro, "Toward Pose-Invariant 2-D Face Recognition Through Point Distribution Models and Facial Symmetry," vol. 2, no. 3, pp. 413–429, 2007.
[11] S. Thavalengal, S. Member, P. Bigioi, S. Member, and P. Corcoran, "Iris Authentication in Handheld Devices – Considerations for Constraint-Free Acquisition," pp. 245–253, 2015.
[12] A. K. Sharma, A. Raghuwanshi, and V. K. Sharma, "Biometric System- A Review," vol. 6, no. 5, pp. 4616–4619, 2015.