World Journal of Research and Review (WJRR)
ISSN: 2455-3956, Volume-14, Issue-6, June 2022 Pages 10-13

A Review Study on Biometric Authentication

Bhawna Kumari, Pooja Gurjar, Ankit Kumar Tiwari

***Abstract*—Advances in the subject of facts technology additionally make data protection the inseparable part of it to be able to address protection, Authentication plays a vital role. This paper presents an assessment of biometric authentication techniques and some destiny possibilities in this discipline. In biometrics, a human being desires to be diagnosed based on a few feature physiological parameters. An extensive style of structures requires dependable non-public recognition schemes to both verify and decide the identification of a character inquiring about their offerings. The cause of such schemes is to make certain that the rendered services are accessed simplest by way of a legitimate consumer, and now not absolutely everyone else. By way of the use of biometrics, it's far possible to confirm or set up a character's identification. The placement of biometrics within the modern discipline of safety has been depicted in this work. We have additionally mentioned opinions approximately the usability of biometric authentication structures, comparisons among different techniques, and their benefits and downsides in this paper.**

***Index Terms*— Authentication, Biometric, Pattern**

I. Introduction

Information security is concerned with the assurance of confidentiality, integrity and availability of information in all forms. There are many tools and techniques that can support the management of information security. But system based on biometric has evolved to support some aspects of information security. Biometric authentication supports the facet of identification, authentication and non-repudiation in information security. Biometrics is the process of recognizing humans from their biological or behavioral traits. Biometric authentication is a type of identification that relies on these human traits to verify a person's identity. It is the most popular form of biometric technology in use today.

The biometric authentication process has three steps: enrollment, recognition and verification. The enrollment step captures the biometric data of a user and stores it in a database. The recognition step compares the captured biometrics to those in the database for verification purposes. And finally, the verification step determines whether or not there is a match between the captured biometrics and those in the database. The most common forms of biometric data are fingerprint recognition, iris scanning and facial recognition.
Such as logging into websites or paying with a mobile device. There are different types of biometrics that can be collected for identification purposes: fingerprints, palm prints, hand geometry (i.e., the shape of a hand), earlobe geometry (i.e., the size and shape of a person's ear).
In this paper, we present a detail survey on Biometric Authentication and we hope that this work will definitely provide a concrete overview on the past, present and future aspects in this field.

Bhawna Kumari, B.Tech Scholar, Department of Computer Science & Engineering, Vivekananda Institute of Technology, Jaipur, Rajasthan.

Pooja Gurjar, B.Tech Scholar, Department of Computer Science & Engineering, Vivekananda Institute of Technology, Jaipur, Rajasthan

Ankit Kumar Tiwari, Assistant Professor, Department of CSE, Vivekananda Institute of Technology, Jaipur

II. Overview

Biometrics (ancient Greek: bios ="life", metron ="measure") refers to two very different fields of study and application. The first, which is the older and is used in biological studies, including forestry, is the collection, synthesis, analysis and management of quantitative data on biological communities such as forests.

Authentication is the act of establishing or confirming something (or someone) as authentic, that is that claims made by or about the thing are true.

III. Detail, Techniques & Technologies

There are quite a few types of identifying a user by way of his own body. Below are the most popular biometric technologies that have made their way into users' hands.

A. Finger Print Technology

There are three types of fingerprint scanners: **optical, capacitive,** and **ultrasound.**

- An **optical scanner** takes a photo of the finger, identifies the print pattern, and then compiles it into an identification code.
- A **capacitive scanner** works by measuring electrical signals sent from the finger to the scanner. Print ridges directly touch the scanner, sending electrical current, while the valleys between print ridges create air gaps. A capacitive scanner basically maps out these contact points and air gaps, resulting in an absolutely unique pattern. These are the ones used in smartphones and laptops.

Fig.1: Fingerprint Bitmap

- **Ultrasonic scanners** will make their appearance in the newest generation of smartphones. Basically, these will emit ultrasounds that will reflect back into the scanner. Similar to a capacitive one, it forms a map of the finger unique to the individual.

B. Face Recognition Technology

A facial acknowledgment method is a utilization of PC for naturally distinguishing or checking an individual from an advanced picture or a video outline from a video source. It is the most regular method for biometric recognizable proof .Facial acknowledgment innovations have as of late formed into two regions and they are Facial measurement and Eigen faces. Facial metric innovation depends on the assembling of the particular facial elements (the framework ordinarily search for the situating of eyes, nose and mouth and distances between these highlights).

Fig.2: Recognition of face from Body

The premise of the Eigen faces technique is the Principal Component Analysis (PCA). Eigen faces and PCA have been utilized by Sirovich and Kirby to address the face pictures effectively. They have begun with a gathering of unique face pictures, and determined the best vector framework for picture pressure. Then Turk and Pentland applied the Eigen countenances to confront acknowledgment issue. The Principal Component Analysis is a strategy for projection to a subspace and is generally utilized in design acknowledgment. A target of PCA is the substitution of associated vectors of huge aspects with the uncorrelated vectors of more modest aspects. Another goal is to ascertain a reason for the informational collection. Fundamental benefits of the PCA are its low aversion to commotion, the decrease of the prerequisites of the memory and the limit, and the expansion in the effectiveness because of the activity in a space of more modest aspects. The methodology of the Eigen faces technique comprises of removing the trademark highlights on the face and addressing the face being referred to as a direct mix of the purported 'Eigen faces' gotten.

Fig.3: Eigen Face.

C. Iris Technology

Iris acknowledgment is an inventive and secure biometric verification technique. Man-made reasoning makes this innovation more available for use in CCTV cameras, cell phones, and other access and security controls. Such ID diminishes the gamble of disappointment of facial acknowledgment frameworks. In this article, we'll cover how the innovation works, an examination of the iris and retina filtering, and the possibilities for the fate of iris acknowledgment. Iris acknowledgment is accepted to have developed from another very notable innovation, retinal confirmation. Iris filtering innovation was first proposed in 1936 by an ophthalmologist, Frank Burch. He expressed that every individual's iris is extraordinary. The likelihood of its occurrence is around 1078, which is a lot higher than with fingerprinting. As per the hypothesis of likelihood, in the whole history of humanity, there have not yet been two individuals with a similar iris. In the mid-90s, John Duffman of Iridian Technologies protected a calculation to distinguish the iris of the eye. Researchers have directed a few investigations demonstrating the way that the human retina can change over the long run while the iris stays unaltered. Observing two totally indistinguishable examples of the eye's iris, even in twins is unthinkable. Glasses and contact focal points, even hued ones, won't influence the imaging system in any capacity. It ought to likewise be noticed that the performed procedure on the eyes, evacuation of waterfalls, or implantation of corneal inserts doesn’t change the iris' attributes; it can't be adjusted or altered. A visually impaired individual can likewise be distinguished utilizing the iris of their eye. However long the eye has an iris, its host can be recognized.

Fig.4: Image of IRIS.

Iris acknowledgment stays one of the most encouraging biometric advances for individual acknowledgment. Particularly sought after is the acknowledgment of the iris' true capacity for use in

non-contact situations ID and a face picture — and potentially other contactless biometric identifiers. Subsequently, the most important exploration bearings are to further develop acknowledgment in painless situations because of further developing sensors, working on the framework's instructive signs, and reconciliation with different modalities. Specifically noteworthy is the utilization of the iris in cryptographic applications and secure recognizable proof. Eye scan recognition has certain advantages over other biometric technologies that make this technology one of the most preferred mobile devices. In recent years, several companies have introduced smartphones equipped with iris authentication technology. Biometric authentication is a promising technology that will eliminate the usual authentication schemes using a password. This will increase the convenience of working with the device, and at the same time, increase the level of protection of personal data.

D. Hand Geometric Technology

Hand calculation is a strategy that connects with the hand mathematical design, which includes finger lengths, finger widths at various areas, palm thickness, palm measurement, and so forth. The job of a normal hand mathematical framework utilizes a camera or scanner-based gadget to catch the hand pictures of an individual. The pictures named layouts are inclined to get highlights, in which a progression of estimations is carried out; models are then positioned in the information base to every one of the clients. Confirmation process is utilized where the info layout is coordinated exclusively with all the data set passages to check an individual's personality. The outcome is the individual might be approved. Hand geometry has many advantages compared to other techniques such that:

1) It needs a camera or moderate resolution reader, which means a medium expense.
2) The fast results produced due to Low computational algorithm.
3) Small template size, which reduces the storage needs.
4) Quite user friendly and appealing resulting in a good acceptance by users.

Neural networks are commonly used for pattern recognition in computational techniques because it has provided high precision in this field. Three types of neural networks were used which are feed forward back propagation, Elman, and the cascade forward neural network.

E. Signature Verification Technique

The signature dynamics recognition is based on the dynamics of making the signature, rather than a direct comparison of the signature itself afterwards. The dynamics is measured as a means of the pressure, direction, acceleration and the length of the strokes, dynamics number of strokes and their duration. The most obvious and important advantage of this is that a fraudster cannot glean any information on how to write the signature by simply looking at one that has been previously written. There are various kinds of devices used to capture the signature dynamics. These are either traditional tablets or special purpose devices. Tablets capture 2D coordinates and the pressure.

Fig.6: A Signature taken using Tablet.

Special pens are able to capture movements in all three dimensions. Tablets have two significant disadvantages. First, the resulting digitalized signature looks different from the usual user signature. Secondly, while signing the user does not see what he or she has already written? He/she has to look at the computer monitor to see the signature. This is a considerable drawback for many (inexperienced) users. Some special pens work like normal pens, they have ink cartridge inside and can be used to write with them on paper.

IV. Discussion

Biometric verification is exceptionally solid, in light of the fact that actual human qualities are considerably more challenging to manufacture then security codes, passwords and equipment keys.
Tokens such as smart card, magnetic stripe cards, ID cards, physical keys, can be lost, stolen, duplicated or left at home. Password can be forgotten, shared or observed. Moreover, today's fast-paced electronic world means people are asked to remember a multitude of passwords and Personal Identification Number (PINs) for computer accounts, banks, ATMs, E-Mail, wireless, phones ,websites and so forth. Biometrics holds the promise of fast, easy, accurate, reliable and less expensive authentication for a variety of application. At the point when Biometric framework is arranged along with telecom innovation, biometric frameworks become Tele-biometric frameworks. The principal tasks are enlistment and test.

V. Conclusion

While biometric authentication can offer a high degree of security, they are far from perfect solution. Sound principles of system engineering are still required to ensure a high level of security rather than the assurance of security coming simply from the inclusion of biometrics in some form.

The risks of compromise of distributed database of biometrics used in security application are high- particularly where the privacy of individuals and hence non-repudiation and irrevocability are concerned. It is possible to remove the need for such distributed databases through the careful application of biometric infrastructure without compromising security.

REFERENCES

[1] R. J. Vidmar. (1992, August). On the use of atmospheric plasmas as electromagnetic reflectors. IEEE Trans. Plasma Sci. [Online]. 21(3). pp. 876—880. Available: http://www.halcyon.com/pub/journals/21ps03-vidmar

[2] Smart Cart Alliance Identity Council (2007): Identity and Smart Card Technology and Application Glossary, http://www.smartcardalliance.org, as visited on 25/10/2008.

[3] Jain, A. K.; Ross, A. & Pankanti, S., "Biometrics: A Tool for Information Security", IEEE Transactions on Information Forensics And Security, Volume 1, issue 2, Jun. 2006, pp 125 – 144.

[4] R. Cappelli, D. Maio, D. Maltoni, J. L. Wayman, and A. K. Jain, ―Performance evaluation of fingerprint verification systems‖, IEEE Trans. Pattern Anal. Mach. Intell., Volume 28, issue 1, Jan. 2006, pp. 3–18.

[5] https://www.biometricupdate.com/tag/iris-recognition

[6] https://www.researchgate.net/publication/335240929_The_New_Hand_Geometry_System_and_Automatic_Identification