International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 09 Issue: 01 | Jan 2022 www.irjet.net p-ISSN: 2395-0072

EMERGING BIOMETRIC AUTHENTICATION TECHNIQUES FOR CARS

Mr.Thippireddy Varun Simha Reddy[1], Mr.Rolla Sai Vignesh Rayal[2], Dr.D.Stalin Alex[3]

[1]Student, Dept. of Electronics & Communication Engineering, Jain University, Karnataka, India
[2]Student, Dept. of Electronics & Communication Engineering, SRM University, Chennai, India
[3]Professor, Dept. of Computer Science & Engineering (Data Science), Jain University, Karnataka, India

---

Abstract - *A Biometric applications have continued to arise since the development of the sensors. The goal of this study is to develop a thorough understanding of biometrics. Biometrics is a phrase that refers to human features, and the fact that it is linked to security makes it even more appealing. By recognising traits that are unique to humans, biometric security makes identity verification easier. More inventions have been produced in this field due to the rapid rise of computer processing. When building a biometric system, the two most critical factors to consider are security and recognition accuracy. Security is essential at our businesses, universities, libraries, laboratories, and many other locations to ensure that our data is kept private and secure from unauthorised access. The lock will open automatically if the fingerprint and facial profile match; otherwise, the password will be requested; if they match, the lock will open. If this happens, the buzzer attached to the audio amplifier will sound to inform everyone close. Biometric authentication plays a key role in delivering high security in automobile door lock systems based on biometric authentication. Today, security is critical to ensure that our data is not kept hidden by unauthorised parties. The major purpose is to secure the automobile, and any car, from unauthorised individuals by employing a unique identifying system that employs biometric authentication. Install a fingerprint scanner, face recognition, and a password to unlock the door, and the door will automatically lock after 30 seconds to give additional security for the owner.*

Key Words: Biometric, Fingerprint, Iris, Voice, Facial, ECG.

1.INTRODUCTION

Vehicle use has grown in importance all over the world, and it is also necessary to maintain it safe from thievery. Carmakers are incorporating security features into their products by using advanced mechanical technologies to avoid thefts, particularly in the event of cars. Biometric and non-biometric solutions provide security highlights. Security frameworks have been seen to crash as a result of stolen secret phrases and decoded information being encrypted, however it is extremely difficult to duplicate distinct characteristics. Biometric frameworks are increasingly commonplace, and technologies such as unique finger impression recognition, iris recognition, and facial recognition are gaining popularity. [1] Fingerprint acknowledgement and discovery frameworks, for example, are simple to convey, current, and persons may be distinguished without their awareness. IThe purpose of an in-car security system is to prevent vehicle theft and ensure the safety of passengers by avoiding the burglary approach.

Recently, the automobile industry has been investing more in computerised advances than at any other time in order to provide improved insight to their customers, particularly with the new directions in Connected vehicles, which provide information both inside and outside the vehicle, and Autonomous vehicles, which require virtually no human involvement in detecting their development and climate. Today, the automobile industry employs an actual validation framework, such as a critical coxcomb, which is vulnerable to theft and tragedy. [11] The goal of this article is to suggest how the automobile industry may use various biometrics to verify and approve their automobiles, and how this can simply expand into providing different outsider administrations while maintaining client security. In this paper, we'll start by illustrating several biometrics, such as fingerprints, faces, hands, irises, retina scans, voice, and ECG, as well as plausible, implementable biometrics for automobiles, before evaluating ideas for biometrics that aren't likely to be as appropriate. Biometric recognition (Biometrics) is based on the recognition of a person's natural and social characteristics. Voice, iris, face, palm prints, finger/palm veins, fingerprints, and voice are just a few examples of biometrics that have been successfully implemented.Such use of biometrics in automobiles might prevent nefarious burglaries in which the owner has left the keys unattended, as well as verifying in-vehicle purchases such as petrol, charges, and espresso or other food-based administrations. [2] Following recognisable proof, the framework will provide customised adaptations, such as seating and backrest alterations, as well as a customised playlist. We can extend the administrations to outsiders with authorisation.

1. BRIEF METHODOLOGY

As shown by Jain et al. Biometrics recognition can be used to verify a person's claimed personality (confirmation mode) or to differentiate a person by comparing the biometric layouts of a large number of characters in a data set for a match (ID mode). The mode is dependent on how the programme is run. In applications like network confirmation, the client asserts his or her identity and proves it by providing a biometric that the framework compares to an all-around enrolled biometric. Confirmation mode is the name given to this mode. The biometric framework operates in distinguishing proof mode by

coordinating the biometric with the known biometrics in reconnaissance actions when hidden tasks are necessary.The phases of a common biometric framework are described, as well as the differences between check and enrollment. [3] Four main parts are envisioned for a biometric framework.

1. Sensor module: The device that records an individual's biometric data. For example, a facial recognition sensor that detects the user's face.

2. Element extraction module: This module analyses the biometric data obtained in order to eliminate a slew of restrictive regulations.

3. Matcher module: Separated pieces are compared to put-away layouts to generate a coordinating score.

4. Framework data set module: This module holds the enrolled clients' biometric forms.

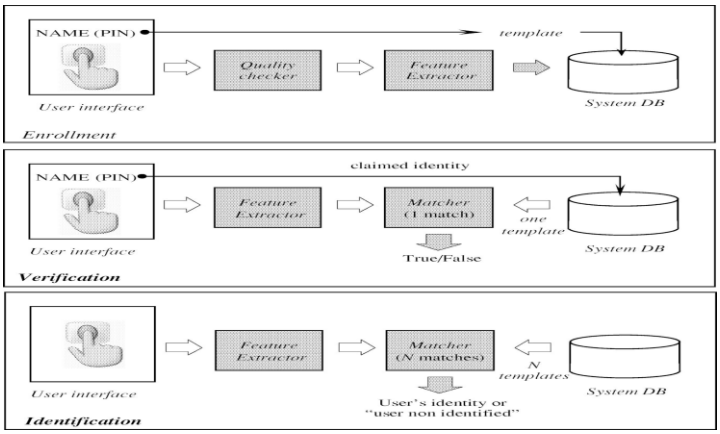

Fig1: Block diagram of enrollment, verification and identification tasks.

Various bio-metrics exist and are utilised in various applications; however, only one out of every odd biometric is appropriate for all applications, and each has its own set of strengths and weaknesses.

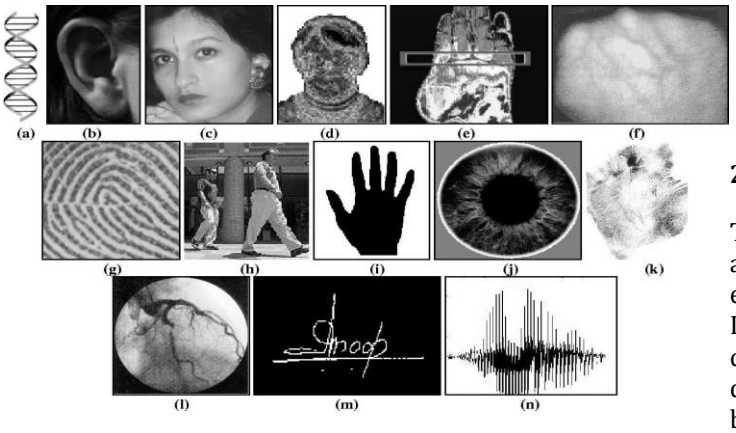

Fig2: Examples of various biometrics

2 Working & Implementation

2.1. Finger print as a bio-metric

Fingerprints are one of the oldest biometrics that is still set up and commonly used by law enforcement agencies who use the "ink-procedure." When a finger is pushed against a sensor, the sensor detects the underlying properties of a unique mark - for example, edges and valleys. The finger imprint design has at least one region, which is referred to as a singularity, and is divided into three types: circle, delta, and whorl. Although the size and cost of unique finger impression scanners have dropped, enabling the employment of innovation for client applications, there are some unique challenges in the management of finger impression explicit photos, such as estimating commotion due to wrinkles, dryness, and wounds.Most unique mark biometrics are now detected by scanning the surface of the finger on a finger imprint scanner. This is known as a "live output." [4] A appropriate sensor to get the biometric is required for live-filter detection. The sensors are usually assigned to one of the three families. Ultrasound, optical, and strong state

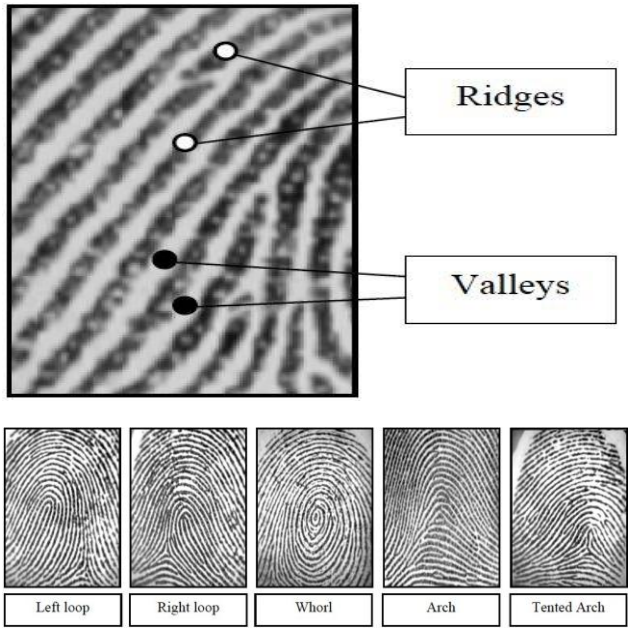

Fig3: Ridges and valleys on a fingerprint.

2.2. Iris as a Bio-metric

The iris of the eye has a surface that may be used to perceive a person. It was initially offered as a strategy for ID based on eye tone and surface, and then developed as a technique for ID based on iris samples. Daugman invented the main camera to capture the iris in the 1990s. It was originally delivered by the UAE for line control in 2001, and it has since been used by countries as diverse as Belgium and the United Kingdom, as well as the United States, India, Mexico, and Indonesia. [5] In their public ID systems, each of them has used the iris. Imaging innovation has accelerated with the

advancement of cameras and imaging sensors. Cameras have gotten more compact and user-friendly. Participation from the subject is essential to capture a photograph; otherwise, the photograph is considered "debased." In 2006, the Iris Moving Framework was introduced, which could capture images of the iris from a distance of 3 metres as the client walked at a speed of 1 metre per second. A-Optix and Delta-ID have made significant advancements in their cameras, and it should now be feasible to do so using a mobile phone. [6]

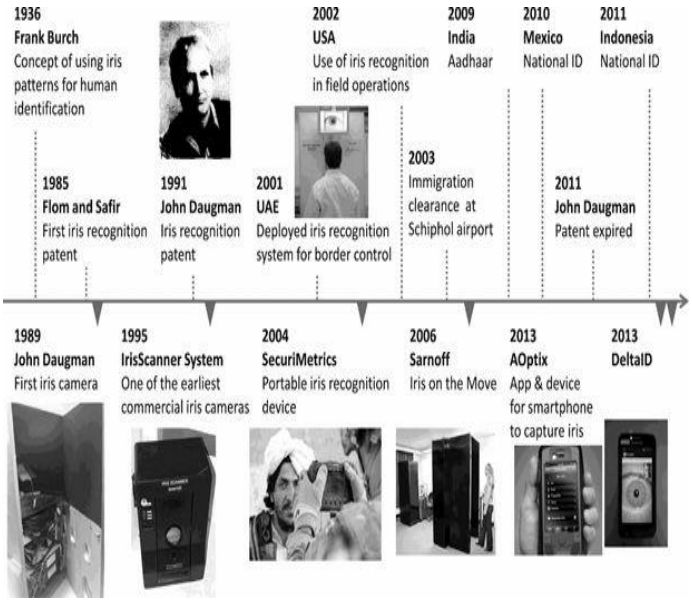

Fig4: Evolution of IRIS biometrics

2.3. Voice as a Bio-metric

The findings of the 2012 NIST Speaker Recognition Evaluation (SRE) reveal a TAR of about 93 percent with a FAR of 0.1 percent. Despite the demanding notion of the NIST SRE 2012 evaluation, which needed the computations to identify if an objective speaker had talked in a specific test discourse fragment with significant foundation turmoil, this indisputable level of precision was achieved. [7] However, the rise of smart speakers such as Amazon Alexa, Google Home, and voice partners such as Apple's Siri and Samsung's Bixby are examples of models that employ speech detecting technology and are similar to those used in the automobile industry for voice instructions.

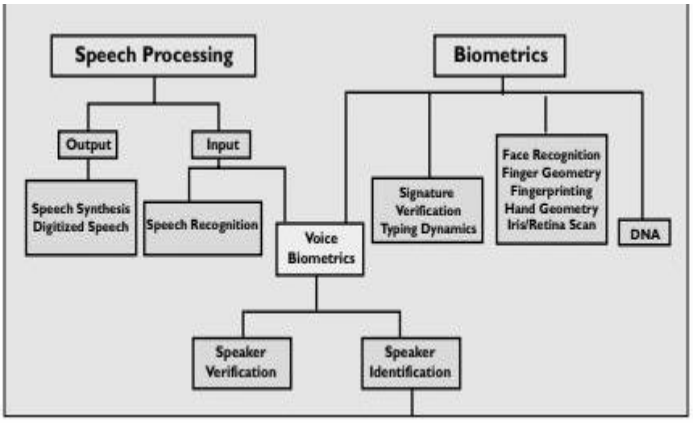

Fig5: Voice recognition model

2.4. Facial Recognition as a Bio-metric

Face is the most often used biometric, aside from finger impressions, because it does not require direct touch or commitment from the customer. Face biometrics plays an important role in areas such as security, access management, and human-robot interaction. [8] The most common use of face biometrics is facial recognition, which is the process of identifying a face from a photograph and comparing it to a pre-programmed framework for determining evidence or confirmation reasons.

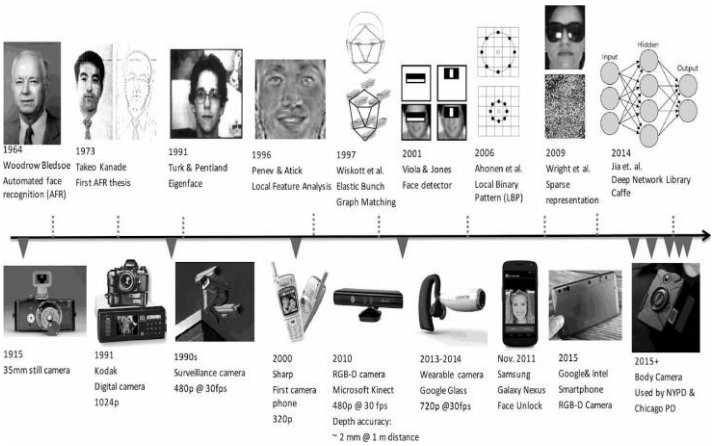

Fig6: Timeline of facial recognition

2.5. ECG as a Bio-metric

Electrocardiogram (also known as ECG or EKG) is a noninvasive method of recording the cardiovascular electrical indications produced by the heart that is also intriguing to everyone. ECG has traditionally been used in the medical field for heart monitoring, but it is now being used in biometrics. [9] Electrical channels, also known as terminals, are placed on the body to measure pulses, which are electrical indications that begin with the depolarization and repolarization of the myocardium, or heart muscle. An ECG signal is a cyclic redundancy with 1-1.5 pulses per second recurrence. P, Q, R, S, and T waves are present in a solid ECG signal [10].

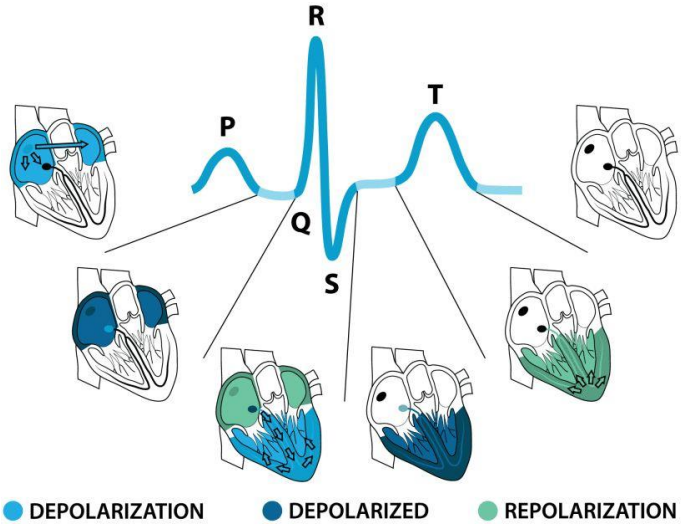

Fig7: The five different wave forms from an ECG signal

3. CONCLUSIONS

Because of the time constraint, our job is limited to a period of thought based on research and information gathered from many examination sources. Fostering this framework and really conducting an evaluation to determine the exactness of the framework, in general, might be considered as future effort. Additionally,[12] a more in-depth examination of employing butt-based biometrics to recognise the client when positioned should be conducted. This biometric technology will be effective in cases when the car owner (under escort conditions) is seated in the secondary lounge and their driver routinely opens and closes the door for them.Similarly, a second technique for verification apart from Biometrics may be necessary at times - either what you know (password) or what you know you have, and these will be useful in situations when Biometrics cannot be provided, such as cuts on fingers. Biometrics in the automobile industry is still in its early stages of development, and it has a wide range of applications. Biometrics' unique characteristics, current advancements in both equipment and calculations, and client acceptance in everyday life create a new client market for associated vehicles.[13] The biometrics frameworks market is expected to be valued at $969 million by 2023.

REFERENCES

[1].A. K. Jain, A. Ross and S. Prabhakar, "An introduction to biometric recognition," in IEEE Transactions on Circuits and Systems for Video Technology, vol. 14, no. 1, pp. 4-20, Jan. 2004.

[2].Apple (2018) Apple T2 Security Chip Security Overview. Retrieved August 16, 2019, from https://www.apple.com/euro/mac/shared/docs/Apple_T2_Security_Chip_Overview.pdf

[3].Robust Iris Recognition in Unconstrained Environments, Journal of AI and Data Mining, A. Noruzi1, M. Mahlouji2, Department of Computer Engineering, Qom Branch, Islamic Azad University, Qom, Iran *and A. Shahidinejad Department of Electrical and Computer Engineering, Kashan Branch, Islamic Azad University, Kashan, Iran. Received 06 September 2018; Revised 22 February 2019; Accepted 08 May 2019

[4].Bhatia, R. (2013). Biometrics and Face Recognition Techniques. International Journal of Advanced Research in Computer Science and Software Engineering, 3(5), pp.93-99

[5].Jain, A., Nandakumar, K. and Ross, A. (2016). 50 years of biometric research: Accomplishments, challenges, and opportunities. Pattern Recognition Letters, 79, pp.80-105.

[6].J. Ribeiro Pinto, J. S. Cardoso and A. Lourenço, "Evolution, Current Challenges, and Future Possibilities in ECG Biometrics," in IEEE Access, vol. 6, pp. 34746-34776, 2018.

[7].I. Odinaka, P. Lai, A. D. Kaplan, J. A. O'Sullivan, E. J. Sirevaag and J. W. Rohrbaugh, "ECG Biometric Recognition: A Comparative Analysis," in IEEE Transactions on Information Forensics and Security, vol. 7, no. 6, pp. 1812-1824, Dec. 2012.

[8].Kulkarni, V. and Babu, V. (2015). Embedded Smart Car Security System on Face Detection. Special Issue of IJCCT, 4(1), pp.112-116.

[9].Santos, Alex & Medeiros, Iago & Resque, Paulo & Rosário, Denis & Nogueira, Michele & Santos, Aldri & Cerqueira, Eduardo & Roy Chowdhury, Kaushik. (2018). ECG-Based User Authentication and Identification Method on VANETs. 119-122

[10].Goodeintelligence.com. (2019). Biometrics for the Connected Car: Identifying Who You Are and How You Are. [online]

[11].Singh, S. (2019). The role of speech technology in biometrics, forensics and man-machine interface. International Journal of Electrical and Computer Engineering, 9(1), 281-288.

[12].R. A. Rashid, N. H. Mahalin, M. A. Sarijari and A. A. Abdul Aziz, "Security system using biometric technology: Design and implementation of Voice Recognition System (VRS)," 2008 International Conference on Computer and Communication Engineering, Kuala Lumpur, 2008, pp. 898-902.

[13].Yang, J. and Xie, S. (2012). New trends and developments in biometrics. Rijeka, Croatia: InTech, pp.149-169.

BIOGRAPHIES

Pursuing B.Tech Final year in Electronics and Communication Engineering at Jain Deemed-to be University, Bangalore as well student member in IEEE.

Pursuing B.Tech Final year in Electronics and Communication Engineering at SRM University, Chennai.

Working as a assistant professor at Jain Deemed-to be University, Bangalore in Computer Science & Engineering(Data Science-Specialization)