Biometric Authentication for Automobiles

Bharath Ratna Karumudi, Phil Gist, Muhammad Qasim Shahzad, Gregory M Wagner

College of Engineering and Computer Science
Syracuse University
Syracuse, NY USA - 13244
(bhkarumu, pjgist, mqshahza, gmwagner)@syr.edu

***Abstract* — Today Biometric technologies are used for identification and verification purposes in many industries and applications to provide secure access. This paper describes on how we can utilize various biometrics for the automobiles, replacing the traditional key fob while integrating other functionalities to enhance the user experience and maintain/enhance security.**

Keywords—Biometrics, Identification, Recognition, Automobile, Connected cars, IoT, Car sharing.

I. Introduction

In recent years the automotive industry has been investing more on digital technologies than ever to provide an enhanced experience to their customers, especially with the recent advancements in Connected cars to provide data both inside and outside the vehicle and Autonomous vehicles.that require little to no human input for sensing its movement and environment.

Today the automobile industry is using the physical authentication system, such as a key fob and which can be prone to theft and loss. The idea behind this paper is to suggest how the automotive industry can use various biometrics to provide the authentication and authorization to their vehicles and how this can evolve into providing various third-party services with ease while maintaining security for their customers.

In this paper, we will start by describing various biometrics such as Fingerprint, Face, Hand, Iris, Retinal Scan, Voice, ECG and suitable, implementable biometrics for cars while reviewing implications with other biometrics that might not be as suitable.

A Biometric based recognition (Biometrics) is based on recognition of an individual's biological and behavioural characteristics automatically. Some examples of successfully implemented biometrics are voice,iris,face,palm prints, finger/palm veins, fingerprints and voice. Such implementation of biometrics in cars could avoid the opportunistic thefts, where the owner has left the keys unattended and also providing authentication for in-car purchases such as gas, tolls, and coffee or other food based services. After identification, the system will provide individualized customizations such as seats and rear-view mirror adjustments, customized playlist. With authorization, we can expand the services to third parties such as in-vehicle deliveries. All this without having either a mobile device or a wallet in hand.

II. About Biometrics

As described by Jain et. al [1] Biometrics recognition can be used to verify their claimed identity (verification mode) or to identify a person by searching the biometric templates of all the identities in the database for a match (identification mode).

The mode depends on the application implementation. In applications such as network authentication, the user claims his/her identity and proves it by giving the biometric which the system compares with an already enrolled biometric. This is referred to as verification mode. Whereas in surveillance operations where secret operations are required, the biometric system runs on identification mode by matching the biometric with the known biometrics. Figure 1[1] illustrates the phases in a typical biometric system and differences between verification and enrollment.

A biometric system is designed with four main modules [1].

1. Sensor module: The device which captures the person's biometric data. For example, a facial recognition sensor that captures the face.
2. Feature extraction module: This module processes the acquired biometric data to extract a set of discriminatory features.
3. Matcher module: The extracted features are compared against stored templates to generate a matching score.

4. System database module: Which stores the biometric templates of the enrolled users.

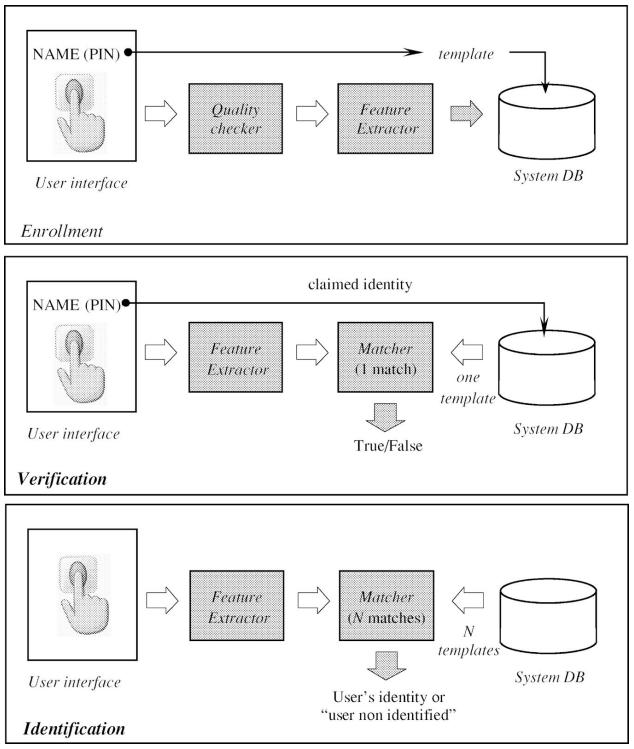

Fig.1. Block diagram of enrollment, verification and identification tasks.

Various biometrics exists and are in use in various applications, but not every biometric is suitable for all applications and each has their own strengths and weaknesses. Figure 2[1] shows various biometrics that are commonly used.

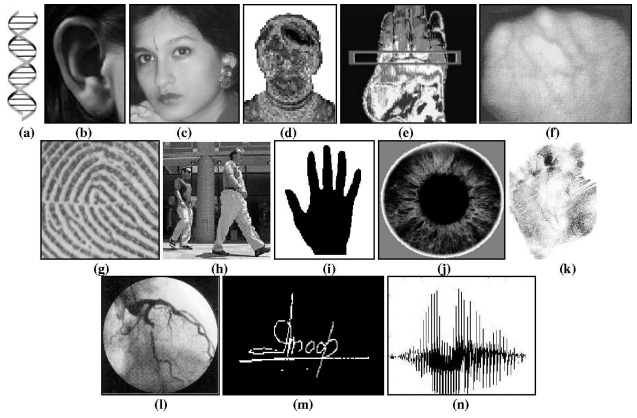

Fig. 2. Examples of various biometrics: (a) DNA, (b) ear, (c) face, (d) facial thermogram, (e) hand thermogram, (f) hand vein, (g) fingerprint, (h) gait, (i) hand geometry, (j) iris, (k) palmprint, (l) retina, (m) signature, and (n) voice.

Measuring the biometric performance

While biometrics helps to improve authentication efficiency, they are also prone to various errors. As such performance metrics are useful to evaluate which biometric to apply to specific applications. Figure 3 shows an example of a performance evaluation on various biometric systems. There are 3 types of performance metrics, Fundamental Performance, Verification System Performance, and Identification System Performance [13].

Fundamental Performance

1. Failure-to-enroll rate (FTE) - The rate at which the system fails to successfully collect data from a biometric sample based upon the user population.
2. Failure-to-acquire rate (FTA) - The rate at which the system is unable to capture a quality biometric sample based upon the number of attempts.
3. False-match-rate (FMR) - The rate at which false matches are made from the matching algorithm for a single template.
4. False-non-match rate (FNMR) - The rate at which false fails are made from the matching algorithm for a single template.

Verification System Performance

1. False reject rate (FRR) - Ratio of false failures made.
2. False acceptance rate (FAR) - Ratio of false positives made.
3. Receiver operating characteristic curve (ROC) - A graph of the FRR vs FAR.
4. Equal error rate (ERR) - The point where FAR and FRR intersect.

Identification System Performance

1. Identification Rate - The ratio of true positives made from the number of identification transactions.
2. False-negative identification-error rate - The ratio of false failures made from the number of identification transactions.
3. False-positive identification-error rate - The ratio of false positives made from the number of identification transactions.

4. Cumulative match characteristic curve - Graph of correct identifications vs rank values.

	False Acceptance Rate	False Rejectance Rate	Crossover Error Rate	Failure To Enrollment	Failure To Capture Rate	Receiver Operating Char.	Sensor Subject Distance
Iris	0.94 %	0.99 %	0.01 %	0.5 %	-	-	30 cm
Retinal	0.99 5	1 %	0.04%	0.8%	-	-	2 cm
Finger Print	2 %	2 %	2 %	1 %	-	-	Zero
Palm Print	-	-	-	-	-	-	Zero
Hand geometry	2 %	2 %	1 %	NA	NA	-	10 cm
Face	1 %	20 %	-	NA	NA	-	~ 20 m
Ear	-	-	-	NA	NA	-	~ 5 m
Shape of X-rayed teeth	-	-	-	-	-	-	50 cm
DNA	-	-	-	-	-	-	Zero
Voice	2 %	10 %	6 %	-	-	-	20 cm
Signature	-	-	-	-	-	-	Zero
Typing rhythm	7 %	0.1 %	1.8 %	-	-	-	Zero

Fig 3. Biometric Performance evaluation table

III. Suitable Biometrics for Automobiles

A brief introduction of biometrics that can be used for the automobile industry.

Fingerprint as a Biometric

Fingerprints are one of the oldest biometrics that are still in place and historically used by law enforcement agencies using the "ink-technique".

When a finger is pressed against a sensor, the structural characteristics of a fingerprint - a pattern of ridges and valleys (refer figure 4[1]) are captured by the sensor. The fingerprint pattern exhibits one or more regions and called singularities and classified into three typologies: loop, delta and whorl (refer figure 5[1]).

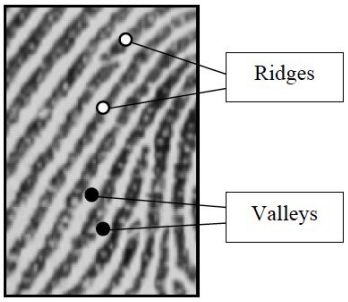

Fig. 4. Ridges and valleys on a fingerprint.

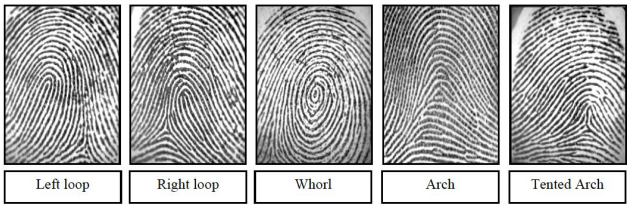

Fig. 5. Five major classes of singularities.

With the recent developments in fingerprint scanners the size and cost has been reduced and enabled the usage of technology for customer applications but still there are some outstanding problems in processing of fingerprint specific images like measuring noise due to creases, dryness and cuts.

In recent days, most fingerprint biometrics are captured directly by sensing the finger surface on a fingerprint scanner. This is referred to as a "live scan". To provide the live-scan sensing, one needs appropriate sensor to acquire the biometric. Typically, the sensors belong to one of the three families [1]: Optical, solid-state and ultrasound as in figure 6[1].

Optical sensors: This is the oldest and most used technique to acquire live-scans. The ridges come in contact with the prism surface and the valleys remain at a certain distance. The light entering the prism is reflected at the valleys and absorbed at the ridges (refer fig. 6a).

Solid-state sensors: In this technique the user directly touches the surface of the silicon plate, where four main effects convert the physical information into electrical signals: capacitive, thermal, electric field and piezoelectric. Small electrical charges are created between the surface of the finger and each of the silicon plates when a finger is placed on the chip (refer figure 6b).

Ultrasound sensors: These work on echography, where sound waves penetrate materials, giving a partial echo at each impedance change. The scanner sends the acoustic signals toward the fingertip and capture the echo signal (refer figure 6c). This echo signal is used to compute the ridge structure. The sensor provides good quality images but is costlier compared to other families.

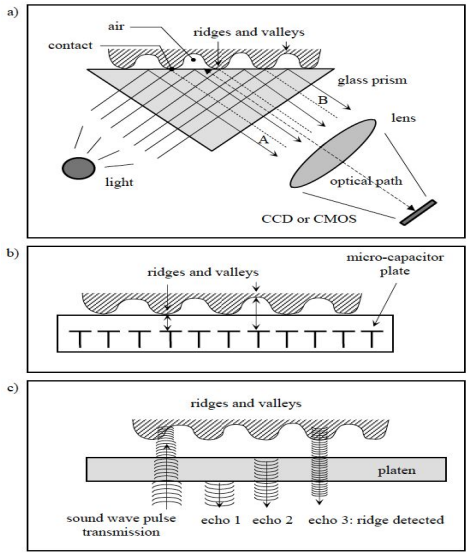

Fig. 6. a) optical fingerprint sensing; b) capacitive sensing; c) ultrasound sensing.

For a car, the optimal place for a biometric sensor is at the door handle to provide the authorization for the driver. As the sensor needs to be exposed to different weather conditions, it will be optimal to use the ultrasound sensor. Another one, on the engine start push button, inside the car to turn on the ignition and will also act as a second layer of authorization to start the car, either a Solid-state or Ultrasound sensor can be used. To provide an enhanced customer experience to the driver with a touchless authentication, an ultrasound sensor can be used.

Fig. 7. User making an authentication to start the car using fingerprint.

Iris as a Biometric

The eye's iris has a texture that can be used in recognizing an individual. It was proposed initially with the use of eye color and texture and then was refined as a method of identification based on the patterns of the iris. In the 1990s the first camera was developed to capture the iris by Daugman. It was deployed initially by the UAE for border control in 2001 and that followed in major countries like Belgium and the UK as well as the USA, India, Mexico and Indonesia. All these have used the iris in their national identification systems.

With the advancement of cameras and imaging sensors, imaging technology in general has grown very quickly. The cameras have become portable and user friendly. To capture an image, the cooperation from the subject is required otherwise the image is considered "degraded". Iris-on-the-move system was introduced in 2006, that could capture images of the iris at a 3m distance with the user walking at 1m/s. Companies like A-Optix and Delta-ID have shown great improvement in their cameras and it can now be done using a smartphone. [4]

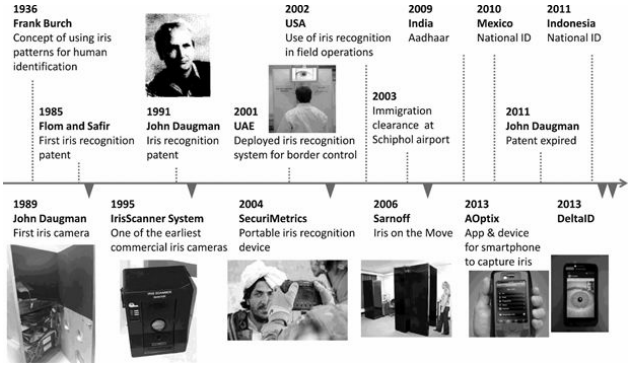

Fig. 8. Evolution of IRIS biometrics

Method for iris recognition:

Figure 9 shows the block diagram for an IRIS biometric system in which the function of each block is briefly discussed as follows:

1) *Image acquisition:* During this stage the image is captured for the IRIS using a camera or an image is gathered from database.

2) *Pre-processing:* The pre-processing of the Iris Image involves the adjustment of contrast, multiplier as well as the edge detection

3) *Segmentation:* The segmentation is done on the iris for the detection of the IRIS itself and the boundaries of the eyelids are eliminated, multiple edge detection methods can be used to find the boundary of the pupil.

4) *Normalization:* The result from the segmentation is converted to a rectangular region from the circular region that will normalize the image of IRIS

5) *Feature extraction:* The image that was normalized is then converted using a filter technique called Gabor filter that will convert it into the binary removing the noise as a result

6) *Classification and matching:* The image template and the image input are now calculated, and shift operations are performed, and decision is made based on the matching score.

Based on the above method, initially a picture is taken of the iris for the car owner and it is stored in a minute database and each time the person approaches a vehicle to validate it will use the above methodology for the iris scanning and matching with the template that is available.

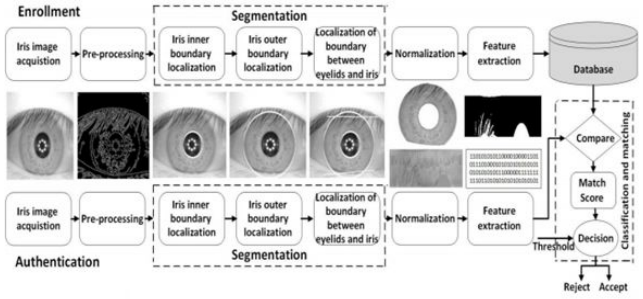

Fig. 9. Overview of Iris Biometric

Performance of IRIS Biometrics

The proposed method [3] similar to the above steps of identity recognition was done on 386 iris images from multiple databases like BATH and CASIA. If there were 2 identical irises, the value would be 0.4. Bigger the value, the decision is easier to make. Consequently, the system success rate equals 98.80% on the CASIA database and is comparable with other methods of IR available utilizing iris images. The failure of 1.2% in iris segmentation stage is due to those images in the database that bear an extremely low color contrast intensity at the border of iris and pupil. The system success rate equaled 97.98% on the BATH database. The reason for this lower accuracy for the BATH database is that the difference of light intensity is extremely low at the border of iris and pupil. FRR and FAR with standard deviation of 0.4, system general accuracy, and the curve relating to relative operating characteristic (ROC) of the proposed method are exhibited in figure 10. Based on this figure, the best threshold value equals 0.4, which results in the error rate of E=0.83%, that is identity acceptance will be done with 98.80% of accuracy. Since each iris has 10 images in database, identity recognition could be done in a way that input image accords at least with N images. ROC curve relating to N = 3, 5, 7, 10 are presented in figure 10. Also, in figure 15, CASIA databases results from the proposed method are shown.

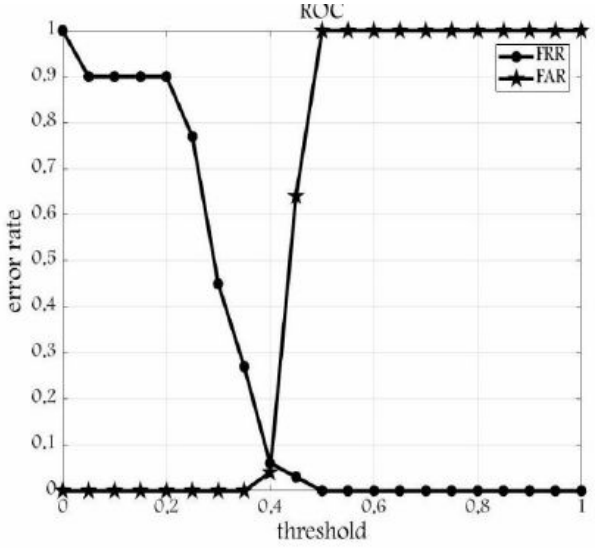

Fig. 10. ROC Curve for IRS

Voice as a Biometric

2012 NIST Speaker Recognition Evaluation (SRE) [5] results show a TAR of approximately 93% at a FAR of 0.1%. This high level of accuracy was achieved despite the challenging nature of the NIST SRE 2012 evaluation, which required the algorithms to detect if a target speaker had spoken in a given test speech segment with significant background noise. Having said that the rise of the smart speakers like Amazon Alexa, Google Home and the voice assistants like Apple's Siri, Samsung's Bixby are some of the examples that use voice sensing technology and similar are utilized in the automobile industry for voice instructions.

Voice biometrics is based on the Speech processing that in turn will be matched with the voice signatures to use it as biometrics. Voice-biometrics systems is categorized as two industries as described in figure 11: speech processing and biometric security.

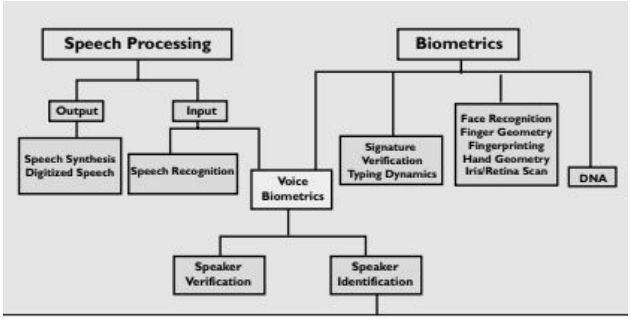

Fig. 11. Voice recognition model

Speech processing: Voice biometrics extracts the information from the stream that is live or captured to accomplish their work. They will use same acoustic that were configured as their closest speech-processing relative speech recognition

Security: The voice biometrics that are used in commercial biometrics that process acoustic information. Most of these commercial voice biometrics systems are designed for use with virtually any PSTN. Standard equipment telephone that is used primarily to support broad deployments of voice biometrics applications in a number of settings.

Function	Application Type	Example
Security	Data and data networks	**BMC Software.** Password reset (over the telephone) using virtual help desk.
		Illinois Department of Revenue. Off-site access to secure data networks.
		INTRUST Bank. Internal wire transfers
	Physical/site access	**U.S. Immigration and Naturalization Service.** Entry to U.S. and Canada during off hours; port of entry at Scobey, Mont.
		Girl Tech. Door access control system and locked box for children.
		City of Baltimore. Evening and weekend access to the five main city buildings.
Fraud Prevention	Telephone network security (toll fraud)	**University of Maryland, College Park.** Toll-free long-distance lines for faculty and staff.
		GTE TSI. Integration of speaker verification into wireless security package offered to carriers.
	Transaction security	**Home Shopping Network.** Automated product-ordering over the telephone.
		Glenview State Bank. Transfer of money between accounts of a bank customer.
Monitoring	Time and attendance monitoring	**SOC Credit Union.** Time and attendance of part-time employees.
		Salvation Army. Time and attendance of Salvation Army workers.
	Corrections monitoring	**New York City Department of Probation.** Tracking of juvenile and adult probationers.
		Dane County Jail, Madison, Wisc. Monitoring of home-incarcerated offenders.

Fig. 12. Examples of deployed voice biometrics

Speaker Verification: Figure 13, shows some of the ways to interact with the speaker-verification system.

Most of the systems that are used rely on the password [11], account information or a pin code that is setup during the initialization, The figure 13 also shows how the voice is used for speech recognition that decodes the input that in turn used by the speaker verification and matched with the voice sample that was stored as a sample. It also shows the text prompted system that asks for random strings to compare the voice samples that were originally stored in the database.

For the system that would be used in the automobile will take the voice input as this example and based on the sample matching for similar words identify the person and may use 2-factor authorization.

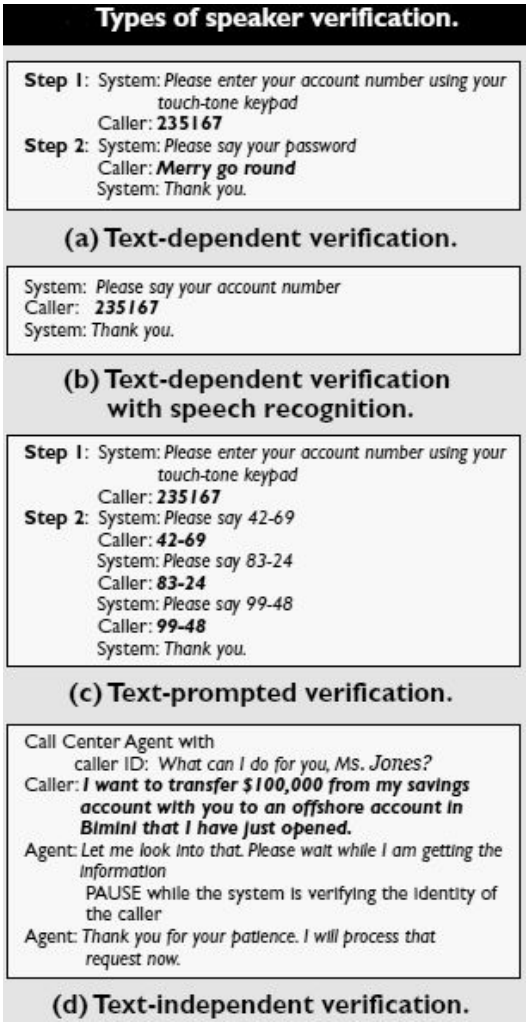

Fig. 13. Types of Speaker Verification

Speaker Identification: Speaker identification activates as soon as a speech is presented that is always text-independent and the system will convert it into a sample voice and compare the sample with the database that exists.[11]

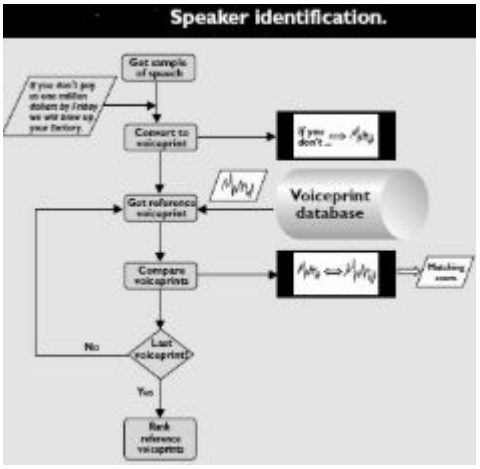

Fig. 14. Speaker Identification

Similar to the Man and Machine interface [11] voice recognition system can be implemented using similar method and can act as an authorization as well as command and control in an automobile.

Performance Analysis of Voice Biometric

There were a couple of experiments done to analyze the performance of a voice recognition system. The other for the accuracy of our own voice [12] and the accuracy of the voice of other people.

During a speaker uttered speech, his/her voice will produce a waveform and known as voice pattern. Every voice pattern is unique and different from other users. Therefore, the first and second experiments are used to analyze the accuracy of the verification process. The accuracy results are shown in figure 15.

Voice Recorded	Voice ID in testing phase (Hz)	Reference voice template in training phase (Hz)	Different between reference voice and voice ID.	*MSE	+Average Pitch	Output
1	0.0995	0.0128	0.0714	0.5864	0.3195	Same User
2	0.0302	0.0128	0.5762	1.2903	0.4667	Same User
3	0.2653	0.0128	0.9518	2.7854	0.5478	Different User
4	0.0509	0.0128	0.7485	0.6627	0.1382	Same User
5	0.0124	0.0128	-0.0323	0.8351	0.3706	Same User
6	0.0742	0.0128	0.8275	1.8257	0.2133	Different User
7	0.0922	0.0128	0.8612	1.7566	0.0589	Different User
8	0.0300	0.0128	0.5733	0.9684	0.0187	Same User
9	0.0310	0.0128	0.5871	0.6477	0.2792	Same User
10	0.0313	0.0128	0.5911	0.7433	0.3094	Same User
11	0.0163	0.0128	0.2147	0.8319	0.4239	Same User
12	0.0742	0.0128	0.8275	0.7759	0.2613	Same User
13	0.0165	0.0128	0.2242	0.5604	0.1976	Same User
14	0.0178	0.0128	0.2809	0.2898	0.3061	Same User
15	-0.1098	0.0128	1.1166	2.1061	-1	Different User
16	0.0299	0.0128	0.5720	0.9905	0.1568	Same User
17	0.2393	0.0128	0.9465	1.4983	0.2853	Same User
18	0.0162	0.0128	0.2099	0.9534	-0.2484	Same User
19	0.2288	0.0128	0.9441	3.0265	0.3137	Different User
20	0.0681	0.0128	0.8120	1.1645	0.1744	Same User

Fig. 15. Voice samples from 20 people were used and MATLAB was utilized to train and evaluate the samples.

Facial Recognition as a Biometric

Outside of fingerprint, face is the most used biometric as it does not require direct contact or participation with the user. Face biometrics plays a significant role in areas such as security, access control, and human robot interaction. The most commonly used aspect of face biometrics is facial recognition, which is the method of detecting a face from an image and comparing that to a trained system for identification or verification purposes. Facial recognition generally consists of 5 steps [12]:

1. *Acquire Image:* This can be captured live or using a photograph.
2. *Locate Image of Face:* Detect faces within the image and crop out remaining image
3. *Analysis of Facial Image:* Take measurements on the face using various algorithmic methods and techniques
4. *Comparison:* Compare image to set of trained images or templates.
5. *Match or No Match:* Determine if the facial image closely matches a stored image.

Woodrow W. Bledsoe and his colleagues at Panoramic Research initiated the work on enabling computers to detect human faces in the mid-1960s, see Figure 16 [5]. This was a semi-automated system as the administrator had to take the facial measurements (distance from ears, mouth, nose, etc) which was then entered into the computer for automatic recognition.

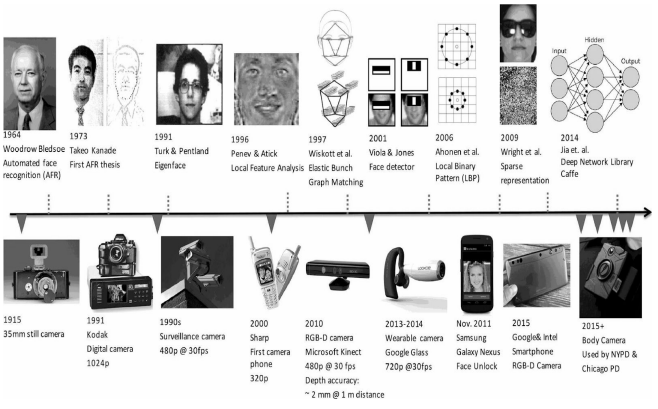

Fig. 16. Timeline of facial recognition

Today, most face recognition techniques assume that the faces will be properly aligned. The alignment is usually based on geometric recognition which is the location of the nose and two eyes on the face. Other

methods of recognition are photometric, which uses skin color and contrast as a form of recognition. Considered a milestone, the face detection scheme developed by Viola and Jones enables faces to be detected in real-time regardless of the presence of background noise, which is a commonly occurring scenario in applications such as surveillance. [5]

Advancements in algorithms have not only helped improve face recognition accuracy, but practical face recognition systems have also improved due to advancements in facial acquisition systems such as infrared, video, 2D (intensity image), and 3D (intensity and depth/range image) camera.

Facial recognition helps to add additional security in the automobile industry, especially for a multimodal system. Two main purposes which make facial recognition a promising biometric for cars, continuous checks to make sure the person driving is the intended driver and the ability to capture a facial image of the person trying to steal the car.

To implement this we would design a system similar to the one used in the research paper by Kulkarni and Babu [8], a low-cost Face Detection System (FDS) (shown in figure 17) that interfaces with the Global Positioning System (GPS) and the Global System for Mobile Communication (GSM) to notify the car owner when and where their car was stolen. Here the intent was to use FDS whenever a car was attempted to be operated when the alarm has been set. A facial recognition sensor is activated to verify the driver, if the facial recognition is false, an alert is sent to the driver and police via an MMS message which includes the location of the car along with the image of the driver.

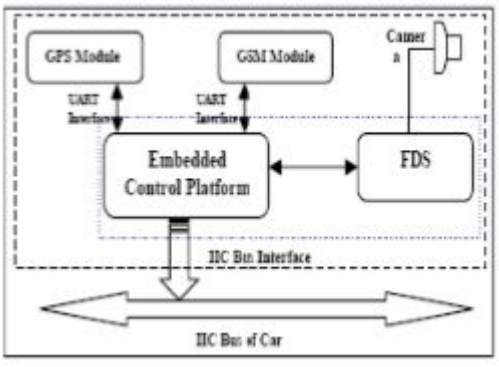

Fig. 17. Model of embedded FDS in car

Our system would expound upon this design to periodically do facial scans to verify the authenticated driver while the car is in motion. The intent is to make sure that a car is not stolen after the authorized driver has opened or started the car. A threshold will be in place that will allow a slotted amount for false rejects before sending an alert to the car owner that the car is potential stolen. This threshold is to compensate for the fact that the driver's face may not be aligned with the camera due to driving conditions (turning head to look at the side view and rear view mirrors). As a bonus, this system will help to mitigate texting while driving as looking down at one's phone will increase the number of false rejects thus triggering car theft procedures. Because there are common driving conditions that can result in an increase in false failures (sunglasses, hat, head turning, etc) an authorized user will have the option of turning off continuous authentication. To do this however, will require authentication such as iris or voice to enable and disable this feature in the infotainment system.

ECG as Biometric

Electrocardiogram (also known as ECG or EKG) trace records the cardiac electrical signals generated by the heart in a noninvasive way that is also unique to each individual. ECG has historically been used in the healthcare sector for heart monitoring, however recently, it is being introduced into biometrics.

To capture ECG data, electrical conductors, as known as electrodes, are placed on the body to measure the heartbeats which are electrical signals originating from the depolarization and repolarization of the myocardium, which is the heart muscle. An ECG signal is a cyclic repetition with a frequency of 1-1.5 heartbeats per second. A healthy ECG signal consists of 5 events P, Q, R, S, and T waves as in Figure 18 [6].

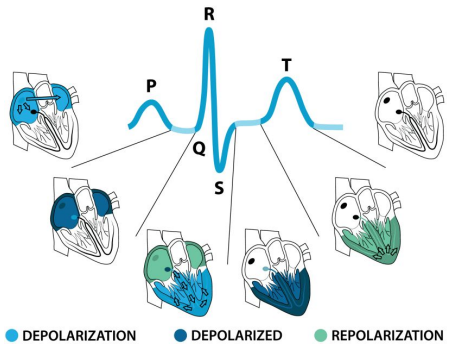

Fig. 18. The five different waveforms from an ECG signal

The ECG signal is characterized by a high degree of variability which is designated into two types intra-subject and inter-subject. Intra-subject is the variation between heartbeat cycles of the ECG of a single subject which is mainly used for health and medical purposes. Inter-subject is the variation between heartbeats of the ECG of different subjects which are useful in biometric recognition. Key factors in both types of variability are:

Heart Geometry: Shape, thickness, size, and shape of the heart are what determines the paths the depolarization of the heart muscle cells.

Individual Attributes: Individual factors such as age and weight can cause shifts in the heart position and/or orientation that will alter the electrical current conduction vectors along the heart.

Physical Exercise or Meditation: Physical exercise or meditation can cause changes in the heart rate which affect the ECG signal.

Cardiac Conditions: Medical conditions dealing with the heart can also cause changes in the dynamics of the ECG signal.

Posture: Different postures such as standing or laying down has an effect on the position of the heart in reference with the electrode placement, thus causing the potential for variations in the ECG signal [6];

Emotions and Fatigue: Psychological states like stress and fatigue can increase or reduce the heart rate, thus affecting the ECG signal.

Electrode characteristics and placement: As with the case with all biometrics the method of collecting data can have an adverse effect on the results. Placement, quality, and size of the electrodes are a few factors that play a part in collecting an ECG signal.

Bielet al., Irvine et al., Kyoso and Uchiyama work helped pioneer identity recognition based on the ECG biometrics [7]. Since then various methods of ECG signal acquisition have been developed:

Medical Acquisitions: The 12-lead ECG configuration is one of the most used configurations, particularly in the medical arena. The 12-Lead configuration allows the acquisition of an ECG signal using 12 electrode leads consisting of three bipolar limb leads, three unipolar limb leads, and six unipolar chest leads [6]. While a well-defined and established method, it is not a practical biometric due to its configuration of leads and limited motion required to obtain the signal.

Movement Freedom and Holter Systems: To progress the collectability of the ECG biometric, methods like the Holter systems were developed to perform acquisitions that allowed the user to perform daily activities while using less electrodes. Acceptance still proved to be minimal as placement of the electrodes are still required on the chest and torso.

Off-the-Person Settings: To improve acceptability and create a biometric system that would be deployed to everyday applications, off-the-person-settings were created to supercede the on-person settings of the two previously mentioned forms of acquisition. Off-the-person settings not only reduced the number of electrodes down to two or three but also relocated the placement of electrodes from the chest and torso to the wrists, hands, or fingers.

Wearables and Seamlessly Integrated Acquisition: With the success of off-the-person settings and the advancement of technology, initiatives have been steered to improve the configurations off-the-person settings by evolving applications into wearable technologies for ECG acquisition and incorporating electrodes into common objects (see Fig. 19)[6].

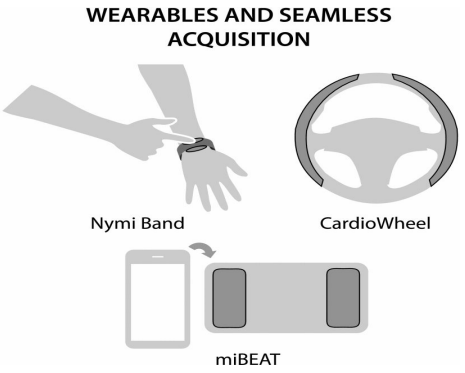

Fig. 19. Wearable and seamless acquisition devices

Like facial recognition, ECG serves two purposes in a multimodal system in cars as it can also be used for authentication but also in driver safety, monitoring the driver for increase in stress, fatigue, or intoxication.

In our system electrode sensors will be placed on the wheel at 10 and 2 o'clock to coincide with the proper way to hold the steering wheel when driving. Before the car is in motion, the system will capture ECG data to verify the driver is an authorized user,

once again further ensuring that the car is not stolen after the car has been started and/or unlocked. A threshold will also be in place to alot for an allotted number of false rejects that can be caused from the driver potentially changing the placement of their hands on the wheel. If the driver fails authentication, an alert via the GSM will be sent to the owner that their car is potentially stolen. A recent study shows that ECG data as a form of driver authentication has a high accuracy rate as shown in the confusion matrix in figure 20 and 21 [9].

Not Driver	Driver	
386	1	Not Driver
17	77	Driver
Accuracy = 96.2578%	Mean absolute error=0.086	

Fig. 20. Confusion Matrix for user authentication process

D1	D2	D3	D4	D5	
98	0	0	0	0	D1
0	95	0	0	1	D2
0	2	82	0	1	D3
0	2	7	81	4	D4
0	0	0	3	105	D5
Accuracy =	95.842%	Mean	absolute error=	0.0357	

Fig. 21. Confusion Matrix for identification using 5 drivers

An additional feature is the safety feature which will continuously take ECG measurements while the car is in motion to compare to the template of the authorized driver. The intent here is to predetermine health conditions of the driver and potentially prevent crashes. The system will alert the driver of a significant changes in their ECG that could be the result of a heart attack, severe fatigue, or intoxication. The user will also have the option of disabling this feature due to conditions that would result in erroneous detections (user wearing gloves, user coming from working out, etc). As with the case for facial recognition the driver will be required to do an authentication in order to disable this feature in the infotainment system.

There are other biometrics such as Gait, Palm and Butt which are also considerable biometrics for automobiles. But due to their limitations in implementation, these are not considered. Gait is a unique biometric but the sensor has to continuously scan for authentication and is very inconvenient to implement in public places, where it has to scan a lot of people. Palm is also a unique biometric but takes a lot of space for the sensor to implement. Recent advancements in this area are showing the improvements in reducing the size of the sensor and one of them is by Fujitsu PalmSecure Palm vein authentication. The other new biometric in the industry and is also best suitable for automobiles is Butt based biometrics, which is also unique but is in initial developments and more research and advancements on this biometric modality are needed.

IV. Implementation Proposal

In this section we will be discussing in detail the implementation of the above discussed Biometrics that are most suitable for automobiles. For connected cars, biometrics are not only for identification but also for in detecting the driver behavior and their wellness. The much suitable biometric modalities for the automobiles are Fingerprint, Face, Voice, and ECG for integration.

There are many applications that biometrics can be implemented for automobiles. These can also enable integrations with services, such as authentication and authorization, with the vehicle. Examples include authorizations to drive the vehicle, providing personalization by identification, wellness monitoring, in-car payments, integrating with insurance companies, home automation and other third-party services.

To protect the vehicle from false proof biometrics, one needs to consider reliable biometric sensors and storage of enrolled biometrics. For instance, we can relate this to Apple usage of the T2 security chip [2] as in figure 22 to store the biometrics in an encrypted format on the storage device.

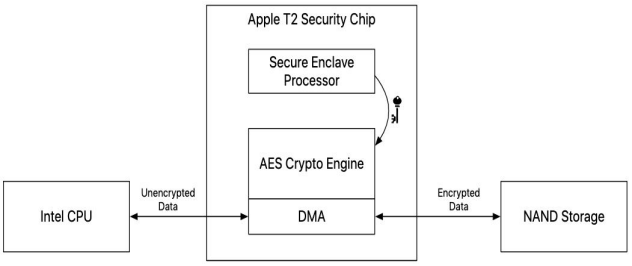

Fig. 22. Apple implementation of processing and storing biometrics

The vehicles would require such a dedicated security chip where registered biometrics will be loaded, processed, stored, purged and to simply provide an API for the applications that ascertain whether the identity is matched with the registered biometrics but not providing access to read any actual stored biometrics. Also, this security chip should be specific to the vehicle to avoid any unauthorized replacement of the security chip with false biometrics. So, an unauthorized replacement will be detected and make the car nonfunctional, until released by the current owner with their biometrics (for resale purposes).

For any biometrics to use, one should first enroll their biometrics. In case of automobiles, when someone is buying a new car from a dealer, the enrollment process will begin during the vehicle delivery. The new owner will be registering his/her biometrics by interacting with the head unit console and the provided sensors. Once the sensors have captured the biometrics, they will be processed and encrypted by the security chip and stored with an assigned primary profile as in figure 23.

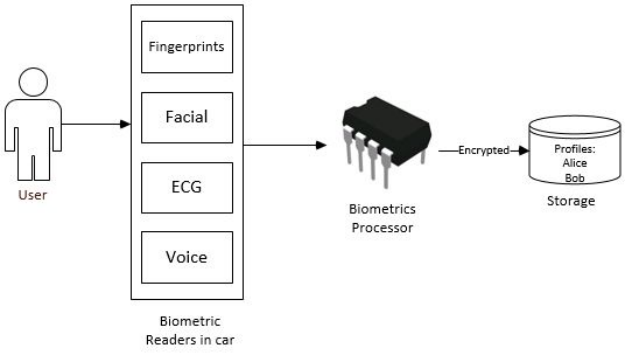

Fig. 23. User registering the Biometrics and profiles creation

The first authentication starts with vehicle entry. Today auto manufacturers are migrating from traditional key to touchless entry to smart device integrations such as mobile phone and wearable devices. But this still depends on external devices, and the security of the car depends on the security of the device. This dependency on external factors can be changed by integrating a fingerprint sensor into the door handles. Such integration will ensure only authorized users gaining entry preventing car thefts and enabling personalization of the car at the same time.

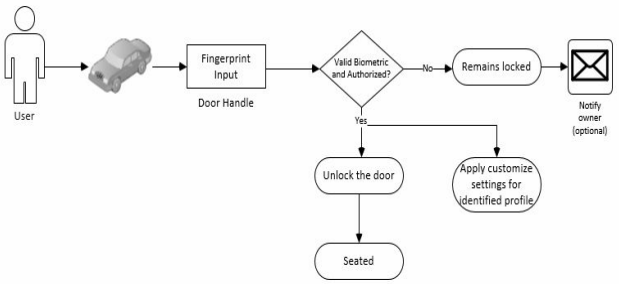

Fig. 24. Block diagram representing user entering into the vehicle

As the biometrics provides identification of the user profile, we can extend this to personalize the car settings as desired. A user can define the settings for seats, rear-view mirrors, music playlist, infotainment systems and save it to his/her profile. During the authentication for gaining access to enter into the car, the profile can be identified and apply the settings. Today the customized settings are available for the driver but not to the passengers, but with the help of Biometrics, the passengers can also register themselves through Biometrics with access only to entry into the car. All this works seamlessly during their first authentication for gaining access.

Once the driver gains access to the car, the next action will generally be an engine start which is a critical authentication and should work all the time flawlessly. Today some automobile manufacturers are providing features to start the engine remotely via an enrolled mobile device, but by using biometrics only the intended user can start the engine. This can be done by integrating the Fingerprint and/or ECG in the steering wheel, and a Face recognition near the driver's console. By implementing two Biometrics that work at one time in providing access and to start a car

will reduce the attack surface and will be difficult for an attacker to hack two different modalities. The other possible biometrics which can be used for this are Voice and Iris.

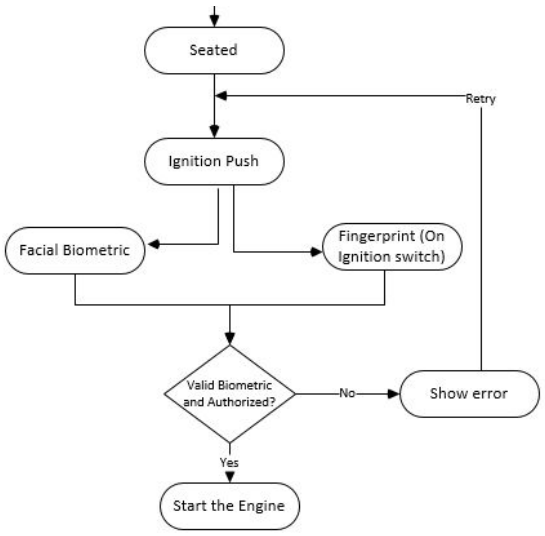

Fig. 25. Turning ON the engine

Today car's infotainment systems are not simply providing entertainment and information, rather they are having capabilities to pay for third party services such as food ordering, fuel payments, toll payments and parking fees. Gas companies like Shell provide a Mobile App and are integrated with specific OEM's infotainment system to pay for the gas from the console. Extending the authorization using the registered profiles, and their corresponding biometrics will provide authorized profiles that can use the in-car payments, rather than anyone who drives the car.

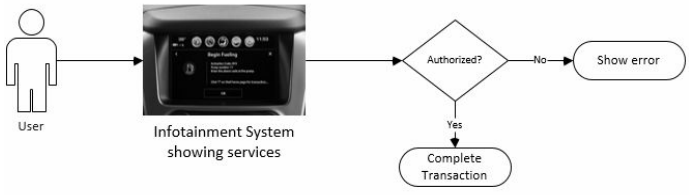

Fig. 26. Using in-car payment services

With the increase in demand of car sharing, we can extend the Biometric based authorization in this area or even to the family members. For this we are proposing a mobile application with a functionality as in figure 27, which is an open platform for all OEMs to integrate. To elaborate this, let's consider Alice is travelling to a new city and Bob is offering his car for rental. Alice likes Bob's offer and sends a request to book the car for her stay in the new city. Alice begins the request from her mobile application and Bob will have either approve or reject the request. If Bob is satisfied with the request, he will send an approval response to Alice and Alice will be authorized to send her Biometrics such as Fingerprint, Facial, ECG that are pre-registered in the app to the authorized car, Over the Air (OTA). The connected car will receive the biometrics from Alice, processed by the dedicated chip and creates a new profile for her in the car with the approved authorizations for the approved amount of time per Bob's approval. The car will send a confirmation to both Alice and Bob about the update. With the proposed approach, the requester's Biometrics will be under requester control and unavailable for anyone to read, except by the authentication system in the car.

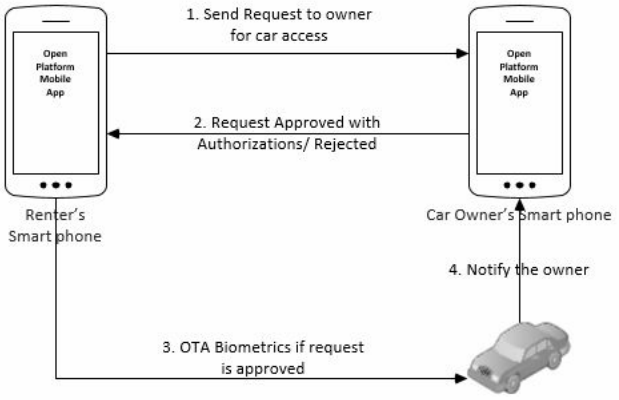

Fig. 27. Car sharing using a mobile app

The above implementation can be extended to in-vehicle delivery services. Where the owner can allow the delivery person biometric to open only the trunk and deliver a package.

The recent adoption of home automation can be integrated and managed from the car while securing the devices such as garage door, thermostats, lights, and home security by authorizing the persons who can operate it. The best suitable biometric is the continuous authentication of driver or voice based, so an authorized passenger can also operate the connected home devices.

Apart from user convenience, the biometric based authentication and authorization can also extend to provide user specific insurance based on driving behaviour, driver's log can be subpoenaed to law

enforcement during crime investigations as well as health monitoring made while driving. The profiles with multiple drivers also help in limiting some functionalities such as setting maximum driving speeds and volume controls.

For two-factor authentication, multiple biometrics can be used to get the authorization for a particular service.

V. Conclusion and Future Work

Due to allotment of time, our work is limited to a phase of concept using studies and data surveyed from various research studies. As future work, developing this system and actually conducting a study to determine the accuracy of the system as a whole could be considered. Also, a more detailed research must be done on utilizing the butt based biometrics to identify the user when seated. This biometric modality will be helpful in the cases where the car owner (chauffeur situations) is sitting in the back seat where their driver generally opens and closes the door for the owner. Also in some cases a second method of authentication apart from Biometrics is needed - either what you know (passcode) or what you have and these will be useful in situations where Biometrics cannot be provided, as an example cuts on fingers.

Biometrics in the automobile industry is still in the research phase and has great opportunities to utilize this proven technology. Biometrics unique characteristics, latest developments in both hardware and algorithms, adoption by users in daily life creates a new user market for connected vehicles. It is estimated that the biometrics systems market will be valued at $969 million by 2023 [10].

VI. Acknowledgment

We would like to express our great appreciation to Professor Gregory M Wagner Ph.D for teaching us Biometrics and providing suggestions during this work. His willingness to give his time so generously was very much appreciated.

VII. 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] Available at: https://www.goodeintelligence.com/wp-content/uploads/2017/11/Goode-Intelligence-White-Paper-Biometrics-for-the-Connected-Car-Identifying-who-you-are-and-how-you-are.pdf [Accessed 16 Jul. 2017].

[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.