Multi-Modal Authentication Systems for Secure Access Control in Autonomous Vehicles

By Dr. Ana Castaño

Associate Professor of Computer Science, University of Buenos Aires, Argentina

1. Introduction

In our work, we propose a secure multi-modal biometric authentication system for access control in autonomous vehicles. It seeks to combine the relatively weak unimodal authentication systems found in unmanned aerial vehicle and autonomous car access control systems into a strong multimodal authentication system. Specifically, the two key areas of focus are on person of interest detection and the adoption of a multi-modal biometric authentication system. The person of interest detection system focuses on the process of detecting a person's existence or entry into access by means of any of the UAV's person sensing modalities. With regard to the multi-modal biometric authentication system, the key areas of focus are on fusing two or more of the autonomous vehicle's biometric devices and on using a customized multi-phased identity verification process.

Multi-modal authentication systems present as enabling secure access control within autonomous vehicles by improving both user identification and verification functions. They adopt a multi-modal concept where features from a combination of unimodal physiological, behavioral, and document-based biometric systems are utilized. This involves a combination of any of the following: physiological and behavioral biometric modalities, physiological or document-based biometric modalities, or document and physiological biometric modalities.

1.1. Background and Significance

To enable a secure distributed decision-making process, we created and tested VehiCoin, a blockchain-based set of smart contracts as a first proof of concept that uses both a voting-based mechanism and multi-modal behavioral profiling data to facilitate the authenticating/behavior diagnostics of the LiDAR, Radar, and Video (LRV) data. Our results demonstrate that not only does a blockchain-based distributed decision-making process

facilitate trusted distributed decision-making, but that the VehiCoin set of smart contracts simplifies behavioral modeling, so responsible behavior across driving situations remains feasible.

The current shift towards autonomous vehicles (AVs) raises challenges concerning how control of the vehicle is decided and verified. As the development of universal loyal guards would make the decision of liability shift from the human controlling the vehicle to the designers of these systems, blockchain technology can build trust towards a distributed set of guardians given the initial trust, while using multi-modal behavioral profiling data to achieve a cooperative distributed decision-making process.

1.2. Research Objectives

To achieve this, three-fold research objectives are drawn: The first research objective aims to create a method that is able to verify that an individual who is actively interacting with the vehicle is a genuine user based on the physiological signals output via user interaction with controlled system parameters. The second research objective will enhance the trustworthiness of the system created by the first research objective. It will do so by generating an individual template repository that is sustainable to random signals. The third objective of this research is to enhance the multi-modal system's user capability by additionally providing a spoofing detector system for hand biometric recognition within in-vehicle scenarios.

Contributions in this research explore and propose the use of multi-modal physiological signals for identity verification within in-vehicle scenarios. These contributions are intended to enhance the security of access control presented by an autonomous vehicle, where an individual having the correct verification can gain access to services. This security enhancement aims to preclude the access to any unauthorized individual regardless of the context: where the context is the physical access to the vehicle or access to specific services.

2. Autonomous Vehicles: Technology Overview

Autonomous vehicles (AVs) have been the subject of many research and development efforts for both related technology and its uses. AVs are expected to improve and provide alternatives in transportation, from reducing congestion and accidents to improving the distribution of resources. However, one of the key challenges that must be resolved to enable or improve the feasibility of AVs to operate in infrastructure-deficient areas, to perform highly secure tasks,

or to act as self-service vehicles employing humans or animals as temporary operators is the secure on-board, remote, and remote-human access control. While many of the challenges and open technical problems relate to the sensing, control, and steering capabilities to navigate obstacles, we suggest that the current status of research activities has generated adequate advances in such areas that suggest solving autonomous vehicle secure access control problems can be addressed in an effective way.

2.1. Key Components and Functions

The eleven-step procedures also preempt and minimize resistance to acceptance and implementation of multimodal biometric terminals, associated logistics, and linking component technologies for conducting evaluations in real-world scenarios.

Close monitoring and the establishment of clear audit trails for the established key functions are also necessary to ensure that security breaches and misuse are detected and reduced to a minimum. This will help distinguish near-behavioral biometric systems from physical and logical biometric systems.

Furthermore, it will ensure fairness, increased performance, and the operational correctness of the authentication system components. Systematic monitoring of the key functions will promote the enforcement and monitoring of multimodal biometric terminals and the supporting logistics policy.

Accurate monitoring of the sequences of the eleven detailed key functions within multimodal biometric authentication systems will result in improved accuracy, reduced error rates, increased tolerance to environmental changes, and the generation of appropriate log messages required for forensic purposes.

In addition, an eleven-step flowchart is presented that highlights the detailed key functions associated with biometrics core components. The flowchart guides technical personnel in the terminal development process, from selecting appropriate biometric modalities to ensuring that multimodal biometric terminals satisfy accuracy, workload, environmental characteristics, accessibility, and security attributes.

At the initial stage, the key biometric components, including input hardware, image capturing and cleaning, feature extraction, data non-repudiation and hashing, data protection, key distribution, stored biometrics, and output matching devices, are discussed.

To develop efficient and reliable biometrics-based authentication systems, a clear understanding of the key components and functions of multimodal biometrics systems is important. A detailed classification of multimodal biometrics systems is also presented in this subsection.

2.2. Challenges and Security Concerns

By presenting fake boxes on the road, the intruder manipulates the autonomous vehicle's steering operations. The designed environment-helping training framework may help attackers create such fake signposts very well, with a 97.3% recognition rate of traffic sign perturbations by convolution neural networks trained with these kinds of adversarial traffic sign images, as reported in. According to, the design of an optimized adversarial image generated to attack autonomous vehicles should be practical for the real world and easily understood physically. The intrusion from the brain-controlled invasive body becomes the driver's area of vulnerability. In an in-vivo non-human model, the vehicle-external communication interface is indirectly attacked.

Typical vehicle subsystems, such as vehicle electronic control units, communication buses, information display systems, vehicle guidance, and navigation systems, and the external cellular interface, are trusted by the external world. Only the driver is supposed to influence the direct control and behavior of the vehicle, supported by the provided HMI and the vehicle user's body. According to, the vehicle HMI security vulnerability becomes the driver's vulnerability. The intruder could weaken the HMI, affecting the automated driving comfort, performance, and endangering vehicle operation. They can affect vehicle guidance and navigation by distorting and driving the mapping information and GPS signal, endangering pedestrians and autonomous driving.

3. Authentication Systems in Autonomous Vehicles

The transition to autonomous driving is anticipated to change humans' interaction with technology. Disengagement from driving will enable occupants to exploit the in-vehicle experience. Consequently, rapid identification of the legally responsible and authorized user

is essential for the realization of secure access. The definition of authorized user status can be determined distinctively by either the ownership of the vehicle, rental or temporary usage of the vehicle, sharing of the vehicle, or assigned guardianship of the vehicle and drivers' unique advantages such as comfort functions and personalized services.

Maintaining security and user privacy in autonomous vehicles is an attractive research area due to the prevalence of inherent security issues that affect user privacy and safety. Endorsing secure recognition of authorized users adds high levels of privacy and security in defining user profiles and assists in the elimination of complex tasks that are essential for maintaining safe and secure driving environments. Genuine assessment of self-awareness or the use of authorized users is crucial as humanized driving functions evolve. Confirmation of user identity can be through different means, including multi-stage checks to reach high recognition levels. Feasibility of and accessibility to the verification mechanism also contribute to what method or means should be used to recognize authorized users. In the quest to reach optimal performance, biometric-based user authentication sets the stage for realizing smart in-vehicle user-facing technologies. The fusion of biometric nodes can ultimately build robust systems for autonomous vehicles that could cope with distinct ambient conditions.

3.1. Single-Modal Authentication

An autocabin may contain a single mode of authentication (like in modern cars with just fingerprint sensors) or multimodal. The different single modes could be fingerprint authentication, speech recognition authentication, facial recognition authentication, gait (manner of walking) biometrics, neural mode biometrics, or an all-in single authentication system which integrates all other single authentication systems. The problem with single modes of authentication in a vehicular environment is that there is a high chance that a student may be able to defeat one single authentication method. If the vehicle can be stolen by using counterfeit, reproduced options or recognized by the car system but with a change in any of the single modalities, then the security level that a car owner or passenger thinks they have is not actual and statistical.

Multi-modality in an authentication system refers to using multiple biometric modalities to obtain data in relation to the unique identity of an individual. Traditionally, biometric systems use a specific sensor for each individual. But rather than using 4 or 5 different biometric authentication systems, it is more secure and inexpensive to employ multiple sensors' data

into a single system for authentication. The level of confidence can be increased for the cabin authentication system with the presence of multi-modal biometrics.

3.2. Multi-Modal Authentication

Additionally, regarding passive physiology from diurnal, biological, and psychological aspects of the human body, these features are generally categorized into permanent-quality biometrics such as fingerprint and iris, non-life intricacy ones like face, gait, voice, and signature, and the liveliness attributes like vein-pattern or ECG biometric signals.

Moreover, MMA can also be extended to the combination of different non-biometric modalities, such as a password and smartcard. Regarding mobiles, which have become more cutting-edge gadgets with redundant design of communication, sensors, and microprocessors, it has been identified that these portable devices have great potential to offer vivid active and passive modalities for user authentication. More and more, it is possible to conduct and access countless services and functionality from mobile equipment due to the development of multi-application or multi-service terminal systems.

Multi-modal authentication (MMA) serves as a robust means of enforcing access to certain functionality or services based on both who the user is and what the user possesses. The two vital factors are presented in one of two different categories: passive and active recognition. Passive recognition is facilitated via biometric identification, while active recognition is typically applied using personalized items like a card, as presented by Jamzad and Ravikiran.

The existing authentication system merely incorporates the identity of authorized users but neglects the assurance of ownership and control over autonomous vehicles. Therefore, the need for multi-modal authentication is obvious, to encompass both areas with the increased access of vehicle configuration parameters such as seating position, driving preference, trip particulars, and vehicle settings.

4. Biometric Modalities for Authentication

Face recognition has become a prominent biometric modality in a variety of applications, including mainly person identification. This technology tends to rely uniquely on the static characteristics of facial identity coefficients, which are much more difficult or impossible to falsify than other types of biometric measurements that rely on dynamic aspects such as

fingerprints or voice. The recently found tremendous progress in face recognition accuracy and reduced training times can be attributed to convolutional neural network (CNN)-based algorithmic developments such as residual networks. Based on their commercial and high resilience to attacks, such as the widely used facial landmark detector library dlib, dlib's ResNet, and various types of VGG Net (Visual Geometric Group). Due to the reduction of several performance parameters, the field of biometric bleaching has been significantly boosted using face recognition. The advantages of CNN-based models in particular for face recognition tasks include reduced processing times for face alignment, reduced face normalization, and efficiency in handling different pose variations.

In order to provide secure, non-intrusive authentication in an autonomous vehicle, multimodal biometric systems can be used to leverage distinct facial and vocal characteristics that provide non-intrusive authentication. Typical modalities that can be used include the use of facial biometric systems incorporating face recognition/verification, voice biometric systems capturing speaker identification as well as speech recognition capabilities to analyze content of the utterance for spoof detection. Additional biometric modalities can potentially be considered such as finger-vein recognizing systems placed on the steering wheel and the gear stick, and hand/finger vein based systems for gesture recognition control.

4.1. Fingerprint Recognition

At present, the two main techniques for fingerprint recognition are minutiae matching and ridge pattern matching. However, there are other distinctive techniques that look for more general data sources, such as sweat gland patterns, pore locations, or mosaic patterns revealed at certain skin growth processes. Since fingerprint scanning has become an organically integrated process in the large units provided for many modern computer environments, along with other security enhancements, they are proposed input systems in the control system for the autonomous vehicle. System integrity can be carefully maintained, provided that due facilitation is given to make the fingerprint reader part of the overall architecture by creating and enabling authentication infrastructure within them.

Fingerprint identification is the oldest method of biometric identification. New techniques in fingerprint acquisition and live-scan sensors have pushed fingerprints into the front row of biometric research. Fingerprints provide a high level of confidence for identifying users and

can be collected covertly. However, sophisticated techniques for fabrication of artificial latent prints enable interested parties to at least attempt to fool the system.

4.2. Facial Recognition

Facial recognition is natural and easy to use, as it leverages the distinctive features on people's faces. It can be done without the user's knowledge or cooperation. In a vehicle, the driver or authorized user can be identified, verified, and tracked using a facial recognition system over a mirror or a screen without stopping the car. The use of deep learning in facial recognition provides an opportunity to achieve stabilized high accuracy on the top-1000 largest person re-identification dataset. It should be noted that the collection and use of facial features to identify and verify individuals pose a major privacy risk. Any collection, transmission, storage, retention, and sharing of biometric data should be in compliance with privacy policies and data protection regulations. Parameters of facial recognition systems should be formally evaluated, tested, and conform to the fairness, robustness, accuracy, and expediency required for specific use cases.

Facial recognition (or face recognition) is a biometric method that uses unique facial features to identify and verify individuals. Facial recognition is a popular biometric that has been used successfully in multimedia and surveillance applications, and is gaining traction in authentication. In designing an authentication system based on facial recognition, the main challenge is the robustness to changes in pose, expression, illumination, occlusion, aging, facial accessories, and mis-registration of sensors. Over the past decade, the study in face analysis has led to the discovery and development of several significant techniques in generative modeling and discriminative modeling.

4.3. Iris Recognition

Iris recognition has been widely accepted as a reliable authentication technique for a variety of environments due to the establishment of ISO/IEC 19794-4 and, above all, BiosecurID that defined evaluation criteria and presented applications requiring automatic pilot authentication. Since the implementation of biometric systems, in particular, the techniques for the detection of individual authentication have been gaining importance because they provide confidentiality, integrity, availability, and non-repudiation in secure communications. For the use of the two characteristics, this implementation requires use that

varies from the safety zone to an autonomous pilot, besides it needs faster responses in its operations.

The acceleration of pattern recognition techniques has made it possible to use fingerprint, face, iris, and also hand geometry technologies for biometric authentication. Among these techniques, palm print recognition works well in cases like iris recognition, where the photo is obtained without the help of the person. This paper raises the use of palm print recognition so that in a situation of an autonomous pilot, it may have access privileges to the resources. For this reason, the focus of this work was to present the use of the biometrics of the palm with applications that need demanding security, like iris recognition, because there is well-tested literature and good reliability.

5. Behavioral Biometrics

Body-based behavioral biometrics is crucial for any implemented or to-be-implemented authentication algorithm for autonomous vehicles. It serves to validate a presence on either side of the transaction occurring inside or outside the vehicle. If the presence can be proven or the face can be verified, the vehicle will become a beacon for both occupants within and outside the vehicle. In case of sleeping, no external activity is detectable and a wake-up signal can be missed. In case of death resulting from an accident, swift intervention must be started at the latest possible time. The car itself serves to protect the space until the emergency services arrive. If an unauthenticated presence persists within the vehicle, it may be necessary to inform the emergency services or the owner in case of illegal activity.

Behavioral biometrics is a young domain in the context of biometric identification, which analyzes biometric information derived from human motion and behavior. This is specifically useful for authentication systems as the body motion information is difficult to steal by an attacker. Motion behavior analysis, though, is not new; it has been mainly discussed in the domain of motion outliers/tester and is, thus far, quite often limited to protecting smart cards, credit cards, or passports. In such systems, this biometric is called "swipe signature." These types of applications usually require additional equipment such as accelerometers or gyroscopes in order to sense the motion. These may be necessary because the motion sensor in many of today's mobile phones has hardware implemented only for the purpose of screen rotation alignment and is not suitable for nor dedicated to this task.

5.1. Keystroke Dynamics

A handful of recent papers have investigated using keystrokes that have been acquired in vehicle-related studies as a potential user performance metric. Ngo et al. considered using keystrokes and smartphone gestures for a discussed repudiation-free solution in motorcars. They leveraged keystrokes and smartphone sensors such as accelerometer, gyroscope, and magnetometer to recognize the genuine vehicle user. They used linear discriminant analysis (LDA), decision tree, SVM, and neural network classifiers to identify the authorized vehicle driver or passenger and observed 88.6% accuracy for keystrokes, 77.6% for touch and gesture, and 93.2% combined accuracy. Rengaraju et al. considered analyzing keystroke timings observed from Microsoft Surface, Dell, and Lenovo laptops to detect data theft. They utilized SVM, k-nearest neighbors (KNN), and LDA classifiers and noted high true positive values.

Keystroke dynamics or typing cadence biometrics use the biometric features available in a person's typing style to assess the authenticity of a key press sequence with the aim to control access to digital sources. Keystroke analysis offers an alternative low-cost, non-invasive, and continuous authentication mechanism, or it could be used to facilitate a strong two-step authentication process. Keystroke analysis systems can analyze dwell time (the time difference between pressing the current key and releasing the previous key), flight time (the time difference between releasing the previous key and pressing the subsequent key), latency time, or key hold time (the time period a key is held before it is released). A machine learning model can be employed to use the information derived from these temporal dynamics, or on user features such as age, gender, and handedness to further refine the user's enrollment process. Although several authentication studies have been conducted on mobile phones and desktop computers, which have mainly focused on pre-defined phrases such as PIN codes, embedded systems such as motor vehicle infotainment and enterprise systems can use time-based features to leverage a few select interaction operations.

5.2. Gait Recognition

A gait recognition system provides continuous user authentication for vehicles. When no action typifying denial of the go-ahead command is verified by systems 1 (biometric as facial recognition) and 2 (vehicle access), the system sends a new set of CAD S2S2 messages to System 1 (biometric as facial recognition) in order to request face photographs, and also new sets of CAD S1S1 and CAD S2S2 messages related with the PPG and WIM sensors,

respectively. Upon determination of the presence of a biometric trait in the user's field of view, which concludes the process with the reference threshold, the system selects the failed biometric trait and runs a new policy. The user may be allowed to access the vehicle depending on the system's conclusion.

The system provides secure access by considering the face as a mask, which is possible in several ways, and not covering enough required immediate time. In summary, to enhance security under different conditions, the fusion of a facial recognition system with a gait recognition system has been applied. The possibility of presenting false biometric information would be considerably reduced. Moreover, by using both modalities as independent methods, it is possible to compartmentalize the risks and behaviors of them.

Consider a user who has left an office having her face covered with a scarf due to severe cold, or a person who is working including circles during the day and wanting to take his/her vehicle using the service of an autonomous valet parking application provided by the 'Autonomous Vehicles' having no access to his/her wallet, cellphone, keys, or any other personal belongings and having his/her face much dirtier than normal. Visage would be closed to the sensors of the vehicle.

The main idea behind gait recognition is to identify a person by the way they walk. The automated recognition of individuals by their gaits is a challenging problem, but presents a low-cost, unobtrusive, and yet reliable biometric option. Besides being a unique trait possessed by each individual, a gait signature is difficult to disguise by costume, makeup, or any other artificial means, and it maintains constant inter-subject signature differences. It is suggested that using gait analysis for recognition is a more reliable method than relying on facial recognition.

6. Fusion Techniques for Multi-Modal Systems

The weighted sum approach: The simplest but most data-inefficient fusion rule, a weighted sum of the preprocessed matching scores or distances taken over the modalities. Simple or heuristic methods are used to optimize these weights by minimizing some loss function over a training set. The basic idea is that the outputs of the various biometrics systems are given different levels of importance, and scores from different biometric systems are combined accordingly to produce a better decision with respect to the actual GT. The rule takes the form

of: Score_albedo = SUM(l,m, wlm x Score_lm), where lm = 1, 2, 3; l = 1, 2, and wlm is an optimized weighting coefficient taken for decision level fusion. The learning phase involves finding optimal coefficients. Two procedures are identified: 1) Score-Level fusion optimized using the Expectation Maximization (EM) method. Under the assumption that distance distributions of impostors derive from a known set of training data, given GTs used to promote a better usage of within biometric distance distribution and Modified Random Projections as a feature selection algorithm.

The goal of output fusion techniques is to combine individual measurements of multiple biometric identification systems to attain better matching performance. There are several techniques in literature for combining the scores from individual matching systems. In fusion techniques, given scores from each individual biometric identification system, a single matching score is developed for each individual by associating with each of the multimodal pair. Once the matching scores are developed for the multimodal pairs, the genuine and impostor scores for the multimodal system are developed, with which the performance of the multimodal system can be assessed. The following sections detail the various well-known fusion techniques.

6.1. Feature Level Fusion

There are times when a decision combination task does not allow for unimodal decisions or weights. A soft decision that is easy to combine for the hardcoded rule can be made. The outputs of a set of recognition experts do not premise that this alone is optimal for the construction of a robust recognition system.

Feature level fusion means transforming the multimodal authentication outputs to a feature space, allowing to operate multimodal representations with generic classifiers. For the decision level fusion method, it provides information about the separate recognitions for all participating modalities. If operational health results fall within a similar operating regime, then the fusion rule is invoked.

Simple fusion methods add the single modal feature into a single combined feature set. Complex fusion methods stack layer multimodal data, then add the layers to the network representation. In this way, it enables the training of multimodal models.

Preprocessing converts multimodal authentication output to a standard feature space. This space can be feature level records from each of the single modalities or combined features from the multimodality records.

Fusion at the feature level comprises combining the features extracted by the individual multimodal modules into a single feature set. A mathematical operation like the concatenation of Gabor and LBP histograms creates a single feature set for preprocessing. It is a fuzzy-based fusion approach that takes into account the appropriate weights for different attributes. Based on the extracted high-level features from the traditional multiple modalities and various decision-level features like extracted outputs, this is an efficiently implemented method that does away with the need for an extensive classifier system.

6.2. Decision Level Fusion

In the decision level – which is a very straightforward technique – the system makes the decision using the results of the devices/sensors instead of combining the feature space, the data, or the robust structures. Nonetheless, some difficulties are encountered in deciding on how the individual outputs of different sensors/devices should be combined in making an optimal multimodal decision. The first step in combining the decisions is to make sure that all the algorithms providing decisions are roughly easy. Indeed, all the individual decisions require equal input to provide similar output. However, they usually do not. Kononenko explained that decision-level techniques are generally post hoc solutions, originated from a great philosophical observation which says that the decision level is a synthesis level, a melting pot of modalities where they all contribute on an equal basis.

Decision-level fusion achieves remarkable improvements in the performance of an IMS system. This is why it is being widely used by the preeminent IMS multimodal systems, e.g., Daugman's famous Biometric Cryptosystem, the fusion-based iris recognition and encryption system. At first sight, someone may think that the decision level technique is antiquated and inefficient. Nevertheless, this is not the reality in many real-world scenarios. In fact, the decision approach can solve plenty of problems that baffle the other levels. Furthermore, the technique is quite simple to implement in software, hardware, and knowledge/machine learning devices.

7. Machine Learning in Multi-Modal Authentication

Other than encryption/decryption, machine learning can be applied in the feature extraction, registration, etc. tasks involved in the ML-aided image processing functions. The IoT sensors installed on-board the vehicles can collect sensory data on various modal of the driver's physiological status. The biometric data encrypted through an initial one-time or community acquisition process. The real-time data needed for access control can then be acquired using the ML-implemented decryption process. The open source software can be employed by the ML developers or the data scientists. The pre-trained deep learning models can be used to compute the scores toward driver authentication. The ML-based multi-modal models can be deployed in two modes for authentication.

These features are employed in the functions of machine learning (ML) models for multi-modal authentication. ML is practically applied in the encryption/decryption of the inputted data and the prediction of the output metrics or labels. In the case of the encrypted biometric data, ML can help in obtaining the access to the features in the data. The open source software like TensorFlow and PyTorch can easily allow for the implementation to the encryption-decryption process. In the AI inference process, the pre-trained artificial neural network is provided to compute the predictions. The output is obtained when the network allows encrypted information to be decrypted by entering the secret key into the network.

7.1. Supervised Learning Algorithms

7.1.1. Random Forest Random Forest (RF) is an ensemble learning method for classification and regression. It constructs a variety of decision trees during training time and trains each tree using a random bootstrap sample. To split the tree nodes during the training time, it searches for the best attribute at every node, which maximizes the reduction of impurities. The top attribute is then selected to represent the splitting decision values. The selection of the top attribute is merged by the majority voting scheme of the trained trees, where each decision tree votes for the final prediction. For regression, it computes the average of predictions. For random forest, the RF classifier applies images with their similarity scores computed from the Siamese network as their training labels in the manner proposed by Lee et al. and directly utilizes the empirical source of attritted fake faces provided by.

Supervised learning algorithm learns from labeled training dataset. When the input features are used to predict output response, the features are known as independent variables and the response is known as dependent variable. Supervised learning falls into two categories:

regression and classification. The output variable for regression data is a real value, such as weight or age in humans, whereas the output variable in classification is categorical, such as red or blue. Supervised learning has been implemented in the proposed research to train the DNN model to recognize different types of fake faces.

7.2. Unsupervised Learning Algorithms

Autoencoders are neural networks commonly used for unsupervised learning. We can consider the avatars obtained with the survival of other drivers during a journey as raw inputs for the neural network. A bottleneck is then in place in the neural networks with the objective function to recreate the inputs at the output layer, using only the ones that survive discretization. After the extraction of the features, the system selects a set of these that deliver disparate outputs, indicating that discrimination is happening in the input options. Additionally, we can segment parts of the trajectory that take place in environments with different semantics in terms of the 3D models.

In unsupervised learning, a system, for example an artificial neural network, is taught to classify inputs according to a statistical quantity of the outputs. One simple use for such technology in the context of multi-model authentication systems is to segment data and provide the apparatus with better inputs. In our case, we can consider unsupervised learning to be a layered security approach where additional inputs can complement the robustness of a security device. Although a number of possibilities exist, we now concentrate our review on the use of unsupervised learning algorithms for leveling the security up in the context of the biometric sensors within the system.

8. Challenges and Future Directions

With the current AV research, there is reliance on the users to have connectivity in order to access centralized data within the vehicle. If an "AV at the edge" is realized, solutions will need to be in place for biometric data security in a decentralized environment. FileUtils will also need to be reengineered to include and process multiple biometric and environmental signals efficiently and effectively. Wear and tear and damage to sensors, the environment and other physical variables will also play a major role in multimodal AS reliability and robustness. These factors will need to be accounted for in future research. Finally, it is essential for multimodal biometric AS for AVs to adopt and include principles generally accepted for

countering spoofing across industries. It is important to note that financial institutions have been able to openly exchange valuable information regarding best practices, new vulnerabilities and next targets through established relationships and forum facilitation. Once multimodal AS are required in physical security access control systems across verticals, industries can share and leverage valuable knowledge and practices.

There are several open research problems that still need to be addressed for multimodal authentication systems (AS) for access control in autonomous vehicles (AV) to become truly viable. Both behavioral biometrics and environmental biometrics are characterized by a high variability between different users of the system. This variability introduces a difficult matching problem that requires sophisticated algorithms tailored to AVs. Additionally, low level and environmental biometrics are sensitive to input data, where noisy or distorted data can severely degrade the robustness of biometric systems. New biometric algorithms and liveness detection techniques will need to be developed to cope with variations in identifying data. Since multimodal biometric AS for secure access control in AVs leverage user intent with physical characteristics to generate an accurate positive user authentication, the possibility of subtle bypass attacks where the user is unaware of the bypass condition are magnified. Researchers will need to develop solutions to recognize when a bypass attack is occurring.

8.1. Scalability and Usability Challenges

Currently, biometric systems are being designed to identify individual operators and use verification to confirm the driver's or hitchhiker's identity. These methods are normally supervised and often only require single capture biometric samples to minimize user cooperation. However, performance drops steeply when authenticating unknown users, often requiring large biometric databases. Experts highly recommend sufficient coverage of environmental variation when employing the face capture modality. It is known that the face modality always identifies all individuals, whereas ear and gait capture are also successful at verifying unknown individuals but require specialized, expensive, high-resolution side sensors and highly identifiable kit or wired internet capture devices. DNA capture is always successful at identifying an unknown passenger, but it is not finished in a timely format for an autonomous vehicle encounter. Keystroke capture is always successful at identifying and verifying an unknown passenger, but it is not feasible for confirming passenger identity, as it applies only to locally operated systems. The liveness test needs to verify the result of all the

biometric capture modality images to avoid negative performance since the smart sensors will fail with unknown false acceptance rate databases. As such, it is not feasible to satisfy the environmental variation.

Autonomous Vehicle (AV) systems are beginning to proliferate. In particular, the necessity to verify passengers (future drivers) or to automatically contact emergency services using trusted means becomes essential to provide trust in self-driving vehicles, as well as to provide the emergency services needed for a wide breadth of non-driving tasks (e.g., sleep, illness, or in the event of a fall). The US Department of Transportation (DoT) defines five levels of autonomy ranging from manual only (No-Automation Level) to partial automation (Function-specific Automation), to conditional automation (Combined Function Automation), to high automation (Limited Self-Driving Automation), to increasing levels of full-self driving automation up to only certain road types (Full Self-Driving Automation) with multi-modal authentication strongly advised for level 5.

Existing multi-modal biometric systems require constant user cooperation to continuously provide samples. In order to enable universal access without user intervention while the vehicle is in motion (e.g., sleep, illness, or in the event of a fall) for autonomous vehicles and to further enhance trust in the vehicle, we introduce an offline access control system. This system verifies a user by conducting a 4D liveness test using user-collected biometric data without the user's explicit consent on resource-constrained devices.

8.2. Emerging Technologies

However, while the tools are made to be lightweight and easy to carry, the authentication process for these wearable devices should also be efficient and transparent enough for the users to utilize. The simplest would be to equip these wearable devices with biometric authentication and access control to enhance the security. The use of multi-modal combinations from the wearables to interface with the wearable device can be the next path to explore for the wearable authentication system. Multimodal biometrics involves the capture of several biometric sources, such as sensors and algorithms, to better interpret face, voice, and fingerprint-based biometrics. These form potentially the richest source of user information for capturing the most human traces under arms-free situations.

The rapid advancement of technology has opened up a plethora of options in the realm of authentication and access control, where a user's identity can be verified precisely in order to circumvent any potential security breaches. Using the same set of technologies on a single device, or combining different modalities, could create the next generation of robust authentication systems. The advantages of using a combined multi-modal authentication system usually include a more accurate result, less possibility of getting a false reject, and better performance. Recent research in authentication systems is taking advantage of emerging new technologies, especially from wearable computing to build useful context-aware applications. Wearable computing can support users in their everyday activities by offering specific content and services based on the context of a particular user. The most attractive advantage of wearable computing is the ability to provide context-aware information and services on-the-fly.

9. References

1. A. Ahmad, M. B. Siddiqui, and R. S. Raw, "Multimodal Biometric Authentication Using Fusion of Fingerprint, Iris, and Face," in 2018 9th International Conference on Computing, Communication and Networking Technologies (ICCCNT), Bangalore, India, 2018, pp. 1-6.

2. R. A. Khan, S. U. Khan, M. I. U. Haq, and S. A. Madani, "A Multimodal Biometric Authentication System Based on Finger Vein, Palmprint and Fingerprint Features," in 2018 14th International Wireless Communications & Mobile Computing Conference (IWCMC), Limassol, Cyprus, 2018, pp. 869-874.

3. N. Kumar, A. Jain, and A. Ross, "Introduction to Multibiometrics," in Handbook of Multibiometrics, Boston, MA: Springer US, 2006, pp. 1-22.

4. Tatineni, Sumanth. "Climate Change Modeling and Analysis: Leveraging Big Data for Environmental Sustainability." *International Journal of Computer Engineering and Technology* 11.1 (2020).

5. Vemori, Vamsi. "Towards Safe and Equitable Autonomous Mobility: A Multi-Layered Framework Integrating Advanced Safety Protocols, Data-Informed Road Infrastructure, and Explainable AI for Transparent Decision-Making in Self-Driving Vehicles." *Human-Computer Interaction Perspectives* 2.2 (2022): 10-41.

6. Venkataramanan, Srinivasan, Ashok Kumar Reddy Sadhu, and Mahammad Shaik. "Fortifying The Edge: A Multi-Pronged Strategy To Thwart Privacy And Security Threats In Network Access Management For Resource-Constrained And Disparate Internet Of Things (IOT) Devices." *Asian Journal of Multidisciplinary Research & Review* 1.1 (2020): 97-125.

7. Vemoori, Vamsi. "Comparative Assessment of Technological Advancements in Autonomous Vehicles, Electric Vehicles, and Hybrid Vehicles vis-à-vis Manual Vehicles: A Multi-Criteria Analysis Considering Environmental Sustainability, Economic Feasibility, and Regulatory Frameworks." *Journal of Artificial Intelligence Research* 1.1 (2021): 66-98.

8. J. Li, X. Yang, Q. Liu, and S. Wang, "Multimodal Biometric Authentication Using Fusion of Palmprint and Finger Vein Features," in 2017 6th International Conference on Computer Science and Network Technology (ICCSNT), Dalian, China, 2017, pp. 335-338.

9. M. U. Javed, M. Hussain, and S. A. Madani, "Multimodal Biometric Authentication Based on Fusion of Palmprint and Iris Features," in 2017 6th International Conference on Computer Science and Network Technology (ICCSNT), Dalian, China, 2017, pp. 303-306.

10. X. Zhao, C. Zou, and Y. Huang, "A Multimodal Biometric Authentication Method Based on Fingerprint and Finger Vein," in 2016 IEEE International Conference on Computational Intelligence and Computing Research (ICCIC), Chennai, India, 2016, pp. 1-5.

11. K. Nandakumar, A. K. Jain, and S. Pankanti, "Fingerprint-Based Fuzzy Vault: Implementation and Performance," in Advances in Biometrics, Berlin, Heidelberg: Springer Berlin Heidelberg, 2005, pp. 310-319.

12. N. Goharian, H. R. Arabnia, and F. M. Fernandez, "A Multimodal Biometric Authentication System Using Fingerprint and Iris Features," in 2009 Ninth IEEE International Symposium on Signal Processing and Information Technology, Ajman, United Arab Emirates, 2009, pp. 147-150.

13. M. E. Kumar, N. K. Jayanna, and V. N. Manjunath Aradhya, "Multimodal Biometric Authentication Using Fusion of Face, Iris, and Fingerprint," in 2015 IEEE International Conference on Computational Intelligence and Computing Research (ICCIC), Madurai, India, 2015, pp. 1-4.

14. D. Zhang, W. Shu, and J. Su, "Hierarchical Fusion of Multiple Palmprint Matchers for High-Accuracy Verification," in IEEE Transactions on Information Forensics and Security, vol. 6, no. 4, pp. 1365-1375, Dec. 2011.

15. L. Chang and W. M. Campbell, "Palmprint Authentication Using Phase-Based Image Matching," in IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 33, no. 6, pp. 1055-1060, June 2011.

16. J. S. Yoo, D. Kim, and J. Kim, "Face Recognition Using Fusion of Near-Infrared and Visible Images," in 2007 IEEE International Conference on Acoustics, Speech and Signal Processing - ICASSP '07, Honolulu, HI, USA, 2007, pp. IV-1349-IV-1352.

17. A. Kumar, A. K. Jain, and S. C. Dass, "Soft Biometric Traits for Personal Recognition Systems," in Advances in Biometrics, Berlin, Heidelberg: Springer Berlin Heidelberg, 2005, pp. 731-738.

18. H. S. Kim, S. Park, and J. Y. Choi, "Personal Authentication System Based on Finger-Vein Patterns," in 2007 11th International Conference on Computer Supported Cooperative Work in Design - CSCWD '07, Melbourne, VIC, Australia, 2007, pp. 649-654.

19. A. Kumar, A. K. Jain, and B. Klare, "Soft Biometric Traits for Continuous User Authentication," in Multimedia Content Analysis and Mining, Berlin, Heidelberg: Springer Berlin Heidelberg, 2007, pp. 731-738.

20. T. Matsumoto, "Impact of Artificial Gummy Fingers on Fingerprint Systems," in Advances in Biometrics, Berlin, Heidelberg: Springer Berlin Heidelberg, 2005, pp. 502-510.

21. N. Ratha, J. Connell, and R. Bolle, "Enhancing Security and Privacy in Biometrics-Based Authentication Systems," in IBM Systems Journal, vol. 40, no. 3, pp. 614-634, 2001.

22. R. Bolle, J. Connell, S. Pankanti, N. Ratha, and A. W. Senior, "Guide to Biometrics," in Advances in Biometrics, Berlin, Heidelberg: Springer Berlin Heidelberg, 2005, pp. 1-27.

23. K. W. Bowyer, K. Hollingsworth, and P. J. Flynn, "A Survey of Iris Biometrics Research: 2008-2010," in Computer Vision and Image Understanding, vol. 115, no. 8, pp. 947-964, Aug. 2011.